HEWLETT® PACKARD

Hands-on, self-paced measurement training guide

Understand your network more completely

Manage your network more efficiently

Troubleshoot more effectively

HP Internet Advisor for Ethernet Training Manual

Note to Users

Hewlett-Packard offers several training choices to the Internet Advisor user ranging from this training manual to structured on-site user certification classes that are offered for each network technology (Ethernet, Token Ring, FDDI, WAN E1 or T1).

The first choice is to get started on the Internet Advisor using this self-paced training manual. This comprehensive collection of exercises will allow new users of the Internet Advisor to learn the product while refining their troubleshooting skills on prepared data files. This manual and the data files that are part of the A.08 LAN software version contain material that has evolved over the last few years from our extensive experience providing user certification classes.

The second option, User Certification classes, is for those who prefer more interactive learning. These classes are led by an HP technical consultant having a background in network technology and troubleshooting. One-day classes are conducted at one of the HP regional training centers or sales offices. To find out more, contact your HP Sales Representative about enrolling in one of the Internet Advisor User Certification classes.

The third choice is to arrange a special, on-site user certification class. Course material can be adapted to take advantage of the opportunity to perform lab exercises on the customer's own local area network.

User certification classes are scheduled by the HP Test and Measurement Education Center, where HP Internet Advisors are set-up in a classroom environment. The class can accommodate up to ten people. Your HP Sales Representative can contact the HP Education Center and arrange for a user certification class to be presented in any city where there is a sufficient number of customer requests. To order, call 1-800-HP-CLASS (1-800-472-5277) in the USA. Outside the USA, contact your local HP sales representative.

In addition, technical support for the Internet Advisor is always available from our Customer Helpline over the telephone (call-back system) or via the Internet.

Customer Helpline: 719-531-4567 in Colorado Springs, Colorado, USA

Internet Address: CCO_HELPLINE@HP-COLSPRINGS-OM1.OM.HP.COM

Plus, please visit our WWW site at: **http://www.tmo.hp.com/tmo/ntd** and then press **Portable Protocol Analyzers**.

Introduction

This training manual is designed to give you a working knowledge of the measurements that can be performed with the HP Internet Advisor for LAN, as well as to provide you with practical applications for using each measurement. Each chapter provides step-by-step instructions on how to configure and run these measurements. The illustrations used are identical to what you will see on your Internet Advisor's screen.

Most measurements described in this manual use data that has been previously captured. However, some measurements will require access to a live network. At the start of each chapter, a section on preparation for the measurement is presented. As you begin a chapter, note whether an Advisor Data File (previously captured data) or a live network, as well as a Node List, is to be used. Loading an Advisor Data File and Node List are detailed in chapter 2.

To fully understand the measurements and capabilities of the Internet Advisor, proceed through each chapter in sequence, and complete all exercises before continuing to the next chapter. This manual is intended to be self-paced. You will gain considerable benefit by performing each measurement that is described. After completing all chapters, use this manual as reference material.

Contents

Manual Conventions

As network measurements are described in each chapter, you are prompted to configure and run the measurement. Text that is **bold** and contained in **[ ]** depicts commands that you should enter on the Internet Advisor. The **|** between commands is for readability only; it should not be entered. For example, if you see **[F4 | Z]**, you should press the **F4** function key and then the **Z** key.

Chapter 1 - Setting Up the HP Internet Advisor for Ethernet

Objective

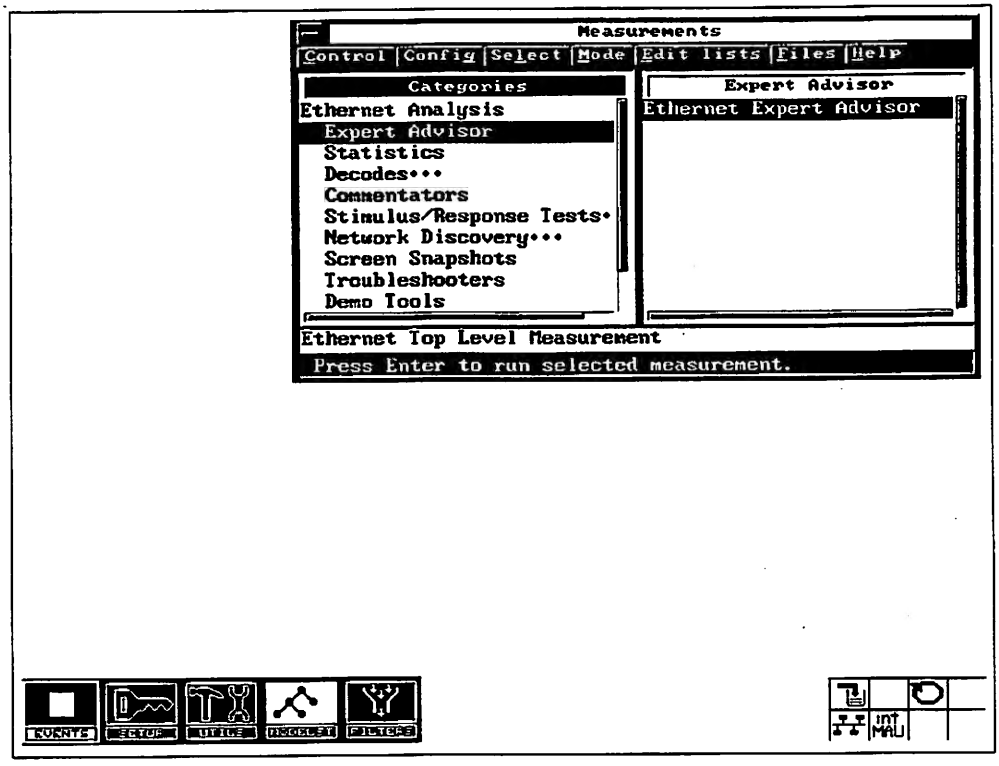
This chapter explains how to configure your Internet Advisor for Ethernet and how to quickly navigate through the instrument's powerful measurement set.

Topics Covered

- Setup window and Status icons
- Additional utilities and configurations
- Controlling the various windows throughout the analyzer
- Event Log and All Events Browser

Preparation

- Internet Advisor for Ethernet should not have any measurements running.
- The Measurements window is properly sized and the categories are fully expanded.



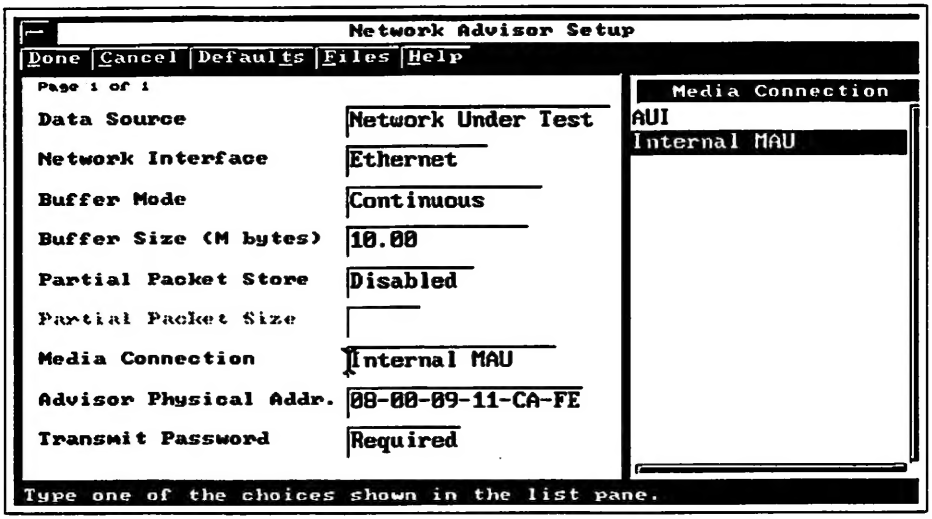
Properly sized Measurements window

Viewing the Setup Window

The Setup window lets you identify the type of network you want to test and how you want the Internet Advisor for Ethernet to operate.

1. Open the Setup window by pressing the **[F9]** Setup key or by double clicking on the **SETUP** icon.

2. Restore default values by selecting **[Defaults | Restore default values]** from the menu bar.



Setup window.

When you open the Setup window, field values are determined by the system setup file. The main areas of the Setup window include:

- Data Source
- Network Interface
- Buffer Mode
- Buffer Size
- Partial Packet Store
- Partial Packet Size
- Media Connection
- Advisor Physical Address
- Transmit Password

To Change a Field Value, Use One of These Methods

1. Position the cursor in a field, select a configuration option from the pane on the right side of the window, and save the values to the system file using the **[Done | Accept changes and exit]** menu bar item.
2. Or, you can load values from a user file, using the **[Files | Load setup/filters from user config file]** menu bar option.

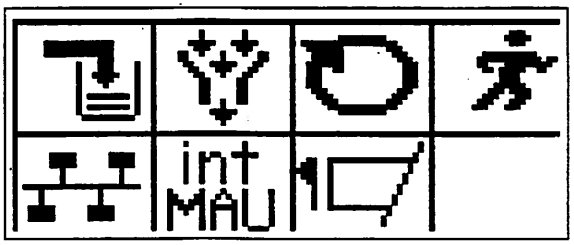
You can undo any changes you make, and you can return the field entries to default values.

- The **Menu Bar** shown at the top of the Setup window includes the following items to control activities for the window.

Item	Activity
Done	Lets you save changes, or save changes and reduce the window to an icon.
Cancel	Lets you cancel any changes you made to the Setup parameters.
Defaults	Lets you restore the original parameter values supplied when the Internet Advisor for Ethernet was shipped.
Files	These options let you save current Setup field values to a user configuration file or the system configuration file, load Setup field values and filters from an existing user or system configuration file, and save the capture buffer to an Advisor Data File. When you save and exit the Setup window, the system configuration file is updated. The next time the Internet Advisor is started, the system configuration file is read and its field values are used as default values.
Help	Lets you access information about the Setup window topics.

There are eight graphic icons in the lower right corner of the Internet Advisor screen. These icons show the current status of the instrument. They can be toggled to change the state of the Internet Advisor. Most of these icons correspond to fields in the Setup window as noted below.

Data Source Capture Filters Buffer Mode Measurements Running



Network Interface Network Connection Partial Packet Store Advisor Busy

- The **Data Source** field in the setup window designates the type of data on which the Internet Advisor for Ethernet will perform measurements. This data can come from an Advisor Data File, the Capture Buffer, or the Network Under Test. This field is disabled when any measurement is running and the Data Source field is Network Under Test.

Item	Activity
Advisor Data File	If you select Advisor Data File in the Data Source field, you can test a previously saved data file in post-processing mode. An Advisor Data File is created when you capture data from the network under test and save it, using the Save Capture Buffer to Advisor Data File in the Setup window Files menu bar option.
Capture Buffer	During a measurement, when Network Under Test is selected in the Data Source field, data from the network under test is stored in the Capture Buffer. If you then select Capture Buffer as the data source, you can re-examine the data just captured from the network.
Network Under Test	Select this when you want to run a measurement on traffic currently occurring on the LAN to which you are connected.

  - ► **Status Icons**—Of the eight graphic icons in the lower right corner of the screen, Data Source is the upper left icon. When Network Under Test is selected in the Data Source field, this icon resembles a buffer filling up with data. When Capture Buffer or Advisor Data File is selected, it resembles a buffer being emptied. You can toggle this setting by clicking on the status icon.

- The **Network Interface** field in the Setup window lets you choose the type of network to test, and your choice affects the measurements you can select to run in the Measurements window. If your Internet Advisor has Ethernet and Token-Ring interface modules, select the appropriate interface to connect to your network under test.

  - ► **Status Icons**—Of the eight graphic icons in the lower right corner of the screen, the Network Interface icon is the lower left icon. When Ethernet is selected in the Network Interface field, the icon resembles several stations connected to a bus.

- The **Buffer Mode** field in the Setup window allows you to save packets in the capture buffer continuously or until the buffer is full.

Item	Activity
Continuous	If you select this before running a measurement, the Internet Advisor initializes the capture buffer, captures data until the buffer is full, then continues to capture data by writing new data over the oldest data in the buffer until you stop the measurement.
Stop When Full	If you select this before running a measurement, the Internet Advisor initializes the capture buffer, captures data until the buffer is full, then stops the measurement.

  - ► **Status Icons**—Of the eight graphic icons in the lower right corner of the screen, the Buffer Mode icon is third from the left in the top row. When you select Continuous capture mode, the icon looks like a circular buffer. When you select Stop When Full capture mode, the icon looks like a linear buffer being filled. You can toggle this setting by clicking on the status icon.

- The **Buffer Size** field in the Setup window lets you specify how much RAM you want to use for the capture buffer. When you select the Buffer Size field, you can choose the maximum or minimum size, or choose one of the specific memory sizes shown. RAM used for the buffer is separate from the 16Mbyte RAM in the 486 PC.

- The **Partial Packet Store** field in the Setup window can be enabled or disabled.

Item	Activity
Enabled	When Partial Packet Store is enabled, the Partial Packet Size field lets you specify the number of bytes in each packet to save. The Internet Advisor captures only the first portion of each packet. By storing only partial packets in the capture buffer, you can store more packets for a given buffer size.
Disabled	When Partial Packet Store is disabled, the Internet Advisor only stores complete packets in the capture buffer. When this field is disabled, you cannot change the Partial Packet Size field value.

  - ► **Status Icons**—Of the eight graphic icons in the lower right corner of the screen, the Partial Packet Store Status icon is third from the left in the bottom row. When the Data Source field is set to Network Under Test, and Partial Packet Store is enabled, the icon resembles a flag followed by a frame of data being truncated. You can toggle this setting by clicking on the status icon.

- The **Partial Packet Size** field in the Setup window lets you specify how many of the beginning bytes of each packet you want to save in the capture buffer. This field is available for selecting choices when the Partial Packet Store field is enabled.

Item	Activity
Bytes to capture	On Ethernet networks, you can capture up to 1518 bytes of each packet. The Internet Advisor for Ethernet uses 32-bit words for the received data. So, the Partial Packet Size value is rounded up so that it is divisible by four. For example, if you enter 41 in the partial Packet Size field and press Enter, the value is set to 44. Default size is 100 bytes. You should not set it lower, or you may slice protocol specific information from the frame, which would adversely affect some measurements.

- The **Media Connection** field in the Setup window is displayed when the Ethernet network interface module is present. This field displays the currently selected media connection and tells the Internet Advisor the connection from which it is to read or send data.

Item	Activity
AUI or Internal MAU	The Internet Advisor can have different physical interfaces depending on the specific product ordered. A LAN only Internet Advisor has a 10Base-T connector and an AUI port, whereas the Ethernet undercradle for the WAN Internet Advisor has a BNC port and an AUI port. The Internal MAU selection captures data from the built-in MAU, either 10Base-T or BNC, and the AUI port captures data from any MAU or AUI cable connected to it.

► **Status Icons**—Of the eight graphic icons in the lower right corner of the screen, the Media Connection icon is second from the left in the bottom row. When the Network Interface field is set to Ethernet, the Data Source field is Network Under Test, and the Media Connection is set to AUI, AUI appears on the status icon. When the Media Connection is set to THINLAN/10base2, internal MAU appears on the status icon. You can toggle this setting by clicking on the status icon.

- The **Advisor Physical Address** field in the Setup window displays the address of the physical layer interface that is currently selected in the Network Interface field. An Ethernet address is displayed when the Network Interface field is set to Ethernet. You can change the physical address field value by typing a value that is not shown in the Physical Address pane. Then when a measurement requires the Internet Advisor to send a source address, it sends that address as the Source Address field contents of a packet. To return the address to the Internet Advisor's actual physical address, select that address from the pane.

- The **Transmit Password** field in the Setup window lets you control the Internet Advisor's ability to run Stimulus/Response Test measurements that transmit on the network. These measurements are listed in the Stimulus/Response Tests Categories in the Measurements window. When you enter the password, all transmit measurements run without requiring the password until the Transmit Password field is reset to Required. The password, "***advisor***" is set at the factory. The Transmit Password state and value are saved to a special location that is read when the instrument boots. If you load a user file that has a different Setup configuration, it will not affect the Transmit Password state and value. Specific states of the Transmit Password field are described below.

Item	Activity
Required	When the Transmit Password is Required, you must enter the password before running a measurement that transmits on the network, such as Traffic Generator.
Disabled	When changing the Transmit Password state to Disabled, you must enter the password. When the Transmit Password state is Disabled, a password is not required to run a measurement that transmits on the network. When changing the Transmit Password state to Required, you can enter any password.
Entered	This state is displayed when you have entered the correct password. When the password has been entered, any transmitting measurement runs without requesting the password again.

► **Changing the Password**—You can change the password by selecting Disabled from the Transmit Password list pane and entering the current password. Then select Required from the list pane and enter the new password. You must enter the password a second time for verification.

Viewing the Function Keys

The function keys (F1-F12) and their actions include:

Key	Activity
F1 Help	Displays information about the currently active window.
F2 Next Window	Selects another window or system window icon displayed on screen.
F3 Next Pane	Selects the next portion of the currently active window.
F4 Window Menu	Selects the activities you can perform on the currently active window. These include zoom, unzoom, icon, move, size, and close.
F5 Close	Closes a currently active window that was activated from a main window. You can close only these types of windows; main windows can only be reduced to icons.
F6	Not Used.
F7 Event Log	Displays the Event Log window. You can then choose to view the protocol, threshold, topology, fault, or instrument events; or you can browse all events.
F8 Meas	Displays the Measurements window, which shows the measurement categories and statistics.
F9 Setup	Displays the Setup window, which lets you select the data source, network interface, buffer mode and size, packet store, media connection, and password requirements.
F10 Utils	Displays the Utilities window, which lets you access the File Manager, the PC hardware configuration, and the autostart configuration; view version information; and exit to DOS.
F11 Node List	Displays the Node/Station List window, which shows all nodes/stations and the information and address for the selected node/station.
F12 Filters	Displays the Capture Filters window, which shows the active filters and allows you to activate and deactivate filters.

You can also use the **Esc** key to toggle between the menu bar and the last window option selected. When using the mouse, you can use the left and right buttons to make selections.

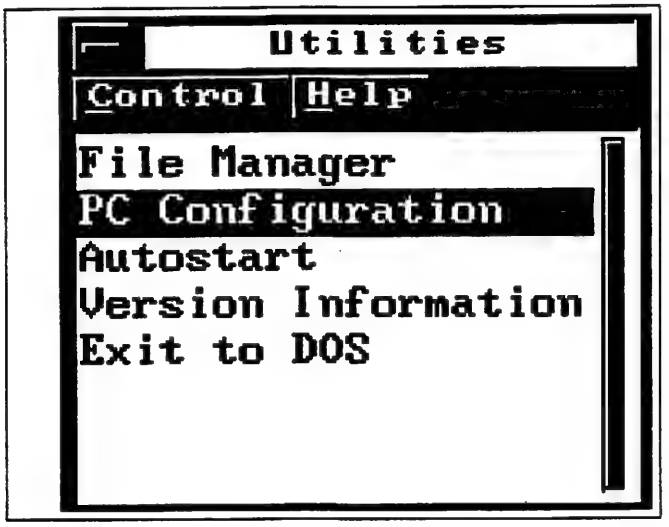
3. Press **[F4 | I]** to iconize the Setup window.

Viewing the Utilities Window

The Utilities window lets you run the following utilities.

- File Manager
- PC Configuration
- Autostart
- Version Information
- Exit to DOS

Press **[F10]** or double click on the **UTILS** icon to open the Utilities window.



Internet Advisor Utilities Window

A summary of each utility follows:

- **File Manager** lets you view the subdirectories and file listings on the hard disk. You can copy, delete, rename, and print files; and create and delete subdirectories. Various data files are included in the \user\datafile subdirectory. Node list storage locations are included in the \user\nodelist subdirectory. The \user\stats directory contains **.csv** files. Other subdirectories in \user are included for autostart, vitals, filters, configuration, setup, and user interface shell files.

- **PC Configuration** shows PC hardware configuration, including type of display, display timeout, type of print screen printer, and whether the print screen output is set to printer, file, or disabled.

- **Autostart** lets you automatically configure or initialize the state of the Internet Advisor, including the PC Configuration, Setup, and Node/Station List windows from either system or user files. You can also automatically run measurements that you select in the Autostart Measurements window; do this after both Enable Configuration and Enable Measurements are selected in the Autostart Configuration window, and after you select and open the Autostart Measurements subwindow.

- **Version Information** lets you view information about the system hardware, firmware, and software version numbers. System version A.08 became available in December, 1995.

- **Exit to DOS** stops all currently running measurements and lets you exit to either DOS or the Internet Advisor Toolkit. Any measurement data not saved will be lost. To restart the Internet Advisor for Ethernet after finishing work at the DOS level, type "***advisor***" at the DOS prompt, or select Ethernet Advisor from the Toolkit menu.

*Note: For more detailed information on the function of any window, use the Help menu to view Help Topics Index for that window. Press **[F1]** for a list of Help Measurement Topics, or from any window, select **[Help]** from the menu bar.*

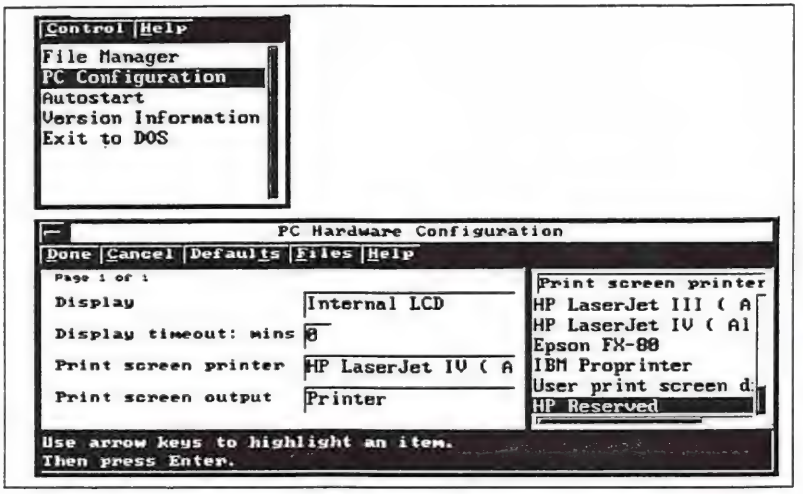
Configure to Print to a Printer or File

1. Press **[F10]** or double click on the **UTILS** icon to select the Utilities window.

2. Select **[PC Configuration]**.

3. Use either the down arrow key or the mouse to highlight the Print screen printer field. Tab to the right and select the appropriate printer, or select HP Reserved to print data to an ASCII file.

4. Use either the down arrow key or the mouse to highlight the Print screen output field. Tab to the right and select Printer if you have a printer attached, or File if you want data from measurements copied to an ASCII file.



PC Hardware Configuration window

5. When finished, select **[Done | Accept changes and exit]**. Press **[F4 | I]** to iconize the Utilities window.

Note: If you do not have a printer directly attached to your Internet Advisor, then configure the Advisor to print to a file. From any measurement that has the Print menu-bar selection, when you select "print", the File Manager application will run and allow you to copy the contents of the measurement to the Internet Advisor's hard drive or floppy drive as an ASCII file.

Using Window Controls

To Activate the Window Menu to Control the Attributes of the Active Window

1. Press **[F9]** to open the Setup window. Press **[F4]**. Then you can:

Select	Then
Zoom	Press Enter to enlarge the window to the maximum screen size.
Unzoom	Press Enter to reduce a zoomed window to its previous size.
Icon	Press Enter to reduce a window to an icon at the bottom of the screen. You can reduce both windows and subwindows to icons. A running measurement that is iconized continues to run.
Move	Press Enter to move the window. When you have positioned the window to where you want it, press Enter again or click the mouse. Or, you can click on the window's title bar and drag the window on the screen.
Size	Press Enter to begin adjusting the size of the window. Use the arrow keys or the mouse to set the window to the size you want. Then press Enter or click the mouse.
Close	Press Enter to close a window. Or, you can use F5 to close a window. Remember, you can only reduce system windows to icons—you cannot close them.

The system windows include Measurements, Utilities, Setup, Event Log, Node List, and Filters.

You can "iconize" system windows. When a system window is iconized, the window reduces to an icon at the bottom of the screen. You cannot use the "Close" menu item to close system windows.

Using Quick Keystrokes

When controlling the attributes of a window, after pressing **[F4]** you can use these shortcuts:

- Press "i" to iconize a window.
- Press "z" to zoom a window.
- Press "m" to move a window.
- Press "s" to size a window.

Internet Advisor Keyboard Shortcuts

Internet Advisor for Ethernet Keyboard Shortcuts		
Function Key	**Label**	**Notes**
F1	Help	
F2	Next Window	
Shift F2	Previous Window	
F3	Next Pane	
Shift F3	Previous Pane	
F4	Window Menu	
F5	Close Window	Can close an iconized window too.
F6	Not Used	
F7	Event Log	
F8	Measurements	
F9	Setup	
F10	Utilities	
F11	Node List	
F12	Filters	
Esc	Menu Bar	A side effect of pulling down the menu bar is that the display pauses.
Tab	Next Pane	
Shift Tab	Previous Pane	

Status Icon Manager			
Data Source	Capture Filters	Buffer Mode	Measurements Running
Capture Buffer or Network Under Test	Activate Capture Filter or Deactivate Capture Filter	Continuous or Stop when Buffer is Full	None—white running man Monitor—black running man Transmit—red running man
Network Interface	Network Connection	Partial Packet Store	Advisor Busy
Ethernet: no selections Token-Ring: 4 or 16 Mbps; participate or non-participate	Internal MAU or AUI	Activate Partial Packet Store or Deactivate Partial Packet Store	Hour glass indicates Internet Advisor is computing. Note: No action is taken when this icon is selected.

Keyboard Accelerators for the Measurements Window in Focus		
Keys	**Operation**	**Notes**
Esc R	Run Measurement	
Esc S	Stop Measurement	
Esc B	Switch to Capture Buffer	This will also stop all running measurements.
Esc O	Run open measurements from network	This will run all measurements that have been opened, including any iconized measurements.
Esc G	Configuration Menu	
Esc M	Format Menu	
Esc T	Print Menu	
Esc H	Help Window	

Keyboard Accelerators for the Window in Focus		
Keys	**Operation**	**Notes**
F4 Z	Zoom or Unzoom the window	Running measurements continue to run.
F4 I	Iconize the window	
F4 M	Move the window	You can also move a window as follows: 1. Click in the window and the title bar will turn yellow. 2. Click and hold on the yellow title bar. 3. Drag the window to the desired location.
F4 S	Size the window	
F4 C	Close the window	Stops a running measurement and closes the window.

Moving Around in the Capture Buffer	
Key	**Function**
Home	Go to first frame in buffer.
Shift Home	Go to start of current frame when in detailed decode. Note: On a PC, use up arrow on number pad.
End	Go to last frame in buffer.
Shift End	Go to end of current frame when in detailed decode. Note: On a PC, use up arrow on number pad.
Down Arrow	Go to next frame in buffer.
Up Arrow	Go to previous frame in buffer.
Right Arrow	Scroll current frame right.
Left Arrow	Scroll current frame left.
Page Up	Scroll current frame up to higher level protocols in frame (detailed decode only).
Page Down	Scroll current frame down to lower level protocols in frame (detailed decode only).
Shift Up Arrow	Scroll up (roll up) one line in current frame to higher level protocols in frame. Note: On a PC, use up arrow on number pad.
Shift Down Arrow	Scroll down (roll down) one line in current frame to lower level protocols in frame. Note: On a PC, use up arrow on number pad.
Enter	Synchronizes decode windows. When running from capture buffer with multiple decode windows open, press Enter to synchronize the decode windows (align all decodes onto the same frame).

Terminating Long Operations	
Key Sequence	**Operation**
Ctrl Break	Stops decode windows that appear hung with an hour glass. The decode is searching for frames that match the protocol decode window.
	Stops capture buffer upload and download (to and from a file).
	Stops decode searching actions.
	Stops printing to printer.
	Stops printing to file.
Alt Ctrl Del	Reboots the Internet Advisor for Ethernet. This is the same as powerup.

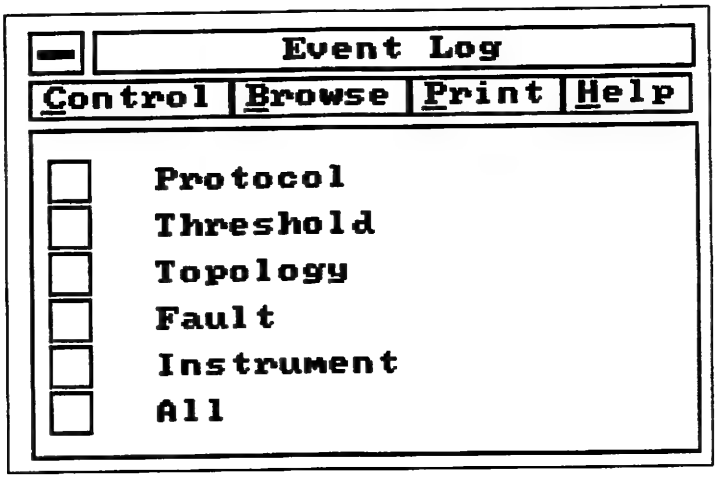
Map of the Internet Advisor for Ethernet

Operation	What's Inside	Function
Measurements	Network Analysis Measurements	Organizes all tools (Statistics, Decodes, Commentators, Stimulus/Response, Network Discovery, Expert Troubleshooters and Snapshots) for analysis of the specified network.
	Expert Advisor	Monitors network and displays network health and other statistics by protocol stack.
	Statistics	Presents a variety of statistical network information.
	Decodes	Displays the contents of the packets on the network.
	Commentators	Summarizes network events at the protocol layer.
	Stimulus/Response Tests	Generates traffic, interact with network devices, and characterize network performance.
	Network Discovery	Displays network configuration, generate baselines, and automatically build a node list including user-given node names.
	Screen Snapshots	Customizes your measurements and screen to create a snapshot.
	Expert Troubleshooters	Integrated measurements to troubleshoot protocol environments.
Setup	Data Source	Selects Network, Capture Buffer, or File as the Data Source.
	Network Interface	Selects the type of network to test: Ethernet or Token-Ring.
	Capture Buffer parameters	Selects Buffer Mode, Buffer Size, and Partial Packet Store.
	Interface parameters	Selects network-specific parameters for Ethernet or Token-Ring.
	Advisor Physical Address	Selects the MAC address for the Internet Advisor for Ethernet.
	Transmit Password	Password protection for measurements which transmit on the network.
Node List		Creates or modifies the node list used by the Internet Advisor for Ethernet.
Filters		Creates hardware capture filters. These filters allow only specified frames into the capture buffer.
Events		Event logs that summarize network events in categories: Protocol, Threshold, Topology, Fault, Instrument, and All.
Utilities		Sets up the printer, manage your disks and files, exit to DOS, and check software version number.

2. Press **[F4 | I]** to iconize the Setup window.

Viewing the Event Log

1. Press **[F7]** to open the Event Log. You can choose to view all events by selecting, from the menu bar **[Browse | Browse All Events]**. The All Events Browser window displays all events occurring on the network under test, along with the date and time the event occurred.



- The Event Log contains six event categories:
  - ► Protocol
  - ► Threshold
  - ► Topology
  - ► Fault
  - ► Instrument
  - ► All

- Each event in the Event Log is categorized:
  - ► "N" indicates a Normal event.
  - ► "W" indicates a Warning event.
  - ► "A" indicates an Alert event.

2. You may print events in the Event Log. Select **[Print]** from any of the six event log categories. You can select to print in text format, or csv format, and choose whether to include normal, warning, and alert events. The Event Log can be printed to a printer or file.

3. Press **[F5]** to close the All Events Browser. Clear the Event Log by selecting **[Control | Clear Event Log]**. A warning appears for verification that you want to clear the log. Select **[Yes]** and press **[Enter]**.

4. Press **[F4 | I]** to iconize the Event Log and press **[F8]** to open the Measurements window.

Chapter Notes

Chapter 2 - Node List and Node Discovery

Objective

Measurements in the Internet Advisor for Ethernet use the Node List as the source for node names, so having an updated node list helps you in troubleshooting and managing your network. Node Discovery and Node List provide valuable tools to help you create one or more node lists. In this chapter, you will learn how to use both the Node Discovery application and the Node List to create one or more node lists that fully document the nodes on your network.

Topics Covered

- File Manager application and its role in managing several different node lists
- An overview on editing node information and adding addresses to the node list
- A discussion of the preferred sequence of passively monitoring the Ethernet network and using the Node Discovery measurement to build an accurate node list
- Creating a node list using buffer data and the replay capability
- In-depth analysis of how the Node Discovery measurement provides results
- Configuring Node Discovery
- Creating, saving, and printing a node list
- Names and Addresses found by Node Discovery

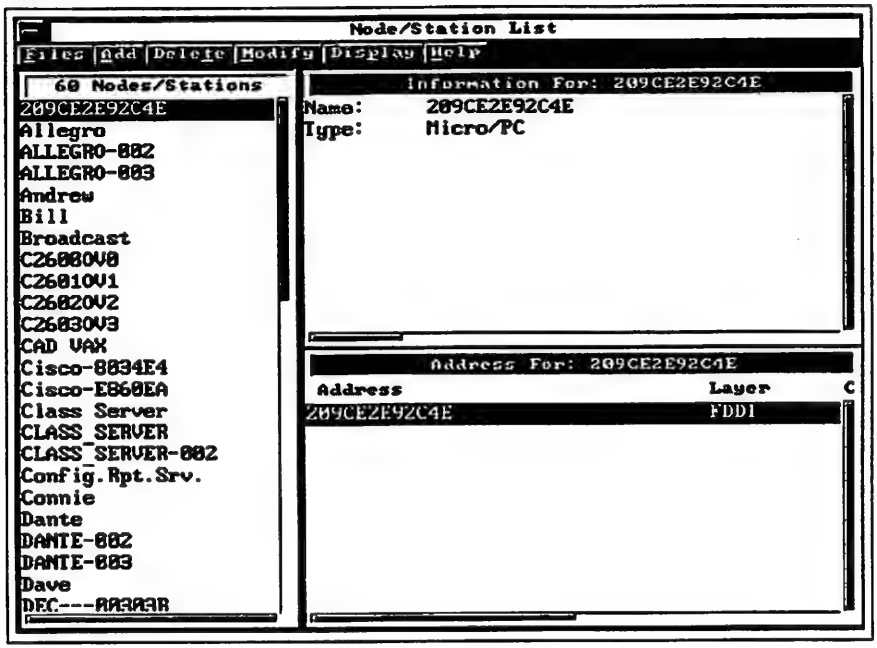
Preparation

- Internet Advisor for Ethernet should not have any measurements running.
- The Measurements window is properly sized and the categories are fully expanded.
- Two Node Lists will be used: **c:\user\class\class.lst** and **c:\user\class\empty.lst.**
- The Advisor Data File **c:\user\class\discover.eth** should be loaded into the capture buffer.

View the Node/Station List Window

1. Open the Node List by pressing **[F11]** or double clicking on the **NODELST** icon.

2. From the menu bar, select **[Files | Load Node/Station List | Replace Node/Station List]**. File Manager opens, displaying Node Lists contained in the ***c:\user\nodelist*** directory. In the Directories pane, change the directory to ***class***. Tab to the Files pane and select **[class.lst]**, then from the menu bar, select **[Done | Accept selection and exit]**. A message appears stating that you will overwrite any existing node list. Select **[yes]** and press **[Enter]** to continue.



Node/Station List with class.lst loaded.

The functions of the Node/Station List window panes include the following:

- All Nodes/Stations
  This pane lists the names of nodes in the current node list according to the current display options.
- Information For:
  This pane shows information about the highlighted node in the node list, including the node name, node type, and any comments. This information could also include the user's phone number, location of the node, and user applications.
- Addresses For:
  This pane shows address information for the highlighted node in the node list, including the address, protocol layer, address name, and cable ID.

Locate a Node in the Node List

1. Select the **[Nodes/Stations]** pane. Type **[sit]** for Site Gateway. The Internet Advisor locates the next occurrence of these letters and displays information about that highlighted node.

Note: Key Word text string search is available in the Node/Station list pane and other lists contained in the Internet Advisor. At the beginning of a list, you may type letters on the keyboard and the Internet Advisor will highlight the first available entry having matching letters. After finding the first occurrence of text, you can use [CTRL] and [F] simultaneously to search forward for the next match, or [CTRL] and [B] simultaneously to search for the previous occurrence. You can find more information about searching in the system Help topics under "searching".

Edit Information About the Node

1. Click twice on the **[Information For:]** pane, or tab to the **[Information For:]** pane and press **[Enter]**. The Node/Station Modification Window is displayed.

2. To edit the node name, click on the **[Node/Station Name]** field.

3. To change the node type, click twice on the **[Node Type]** field, or use the down arrow key to select the **[Node Type]** field.

4. The Comments window is used for entering location information, user phone number, etc.

5. When you have finished, select **[Cancel | Cancel changes and exit]**.

Edit the Node Address

1. From the Node/Station List window, click twice on the **[Addresses For:]** field, or tab to the **[Addresses For:]** field and press **[Enter]**. The Address Editor window opens. You can change the protocol layer, address, cable ID, and address name.

2. When you have finished, select **[Cancel | Cancel changes and exit]**.

Save and Load a Node List

In the Node/Station List window, the Files menu allows you to save and load a Node/Station List. You can define and save multiple node lists on the hard disk.

Save a Node List

1. In the Node/Station List window, select **[Files | Save Node/Station List]** from the menu bar. The Save Node/Station List window opens. The default directory is ***c:\user\nodelist***.

2. Type the name of the new node list in the **[File name:]** field. Maintain the ***.lst*** extension. For this chapter, use the following file name: **[chap2.lst]**

3. From the menu bar, select **[Done | Accept selection and exit].**

Load a New Node List

1. In the Node/Station List window, from the menu bar, select **[Files | Load Node/Station List | Replace Node/Station List]**.

If you elect to replace the Node/Station List, the existing list will be removed from the CURRENT.LST area but will still remain on the hard disk (if previously saved node list file). If you elect to merge the new Node/Station List, the Internet Advisor will combine that list with the currently loaded list.

2. From the File Manager window, select **[c:\user\class\class.lst]**. From the menu bar, select **[Done | Accept selection and exit]**.

When you load a new node list using the replace option, the following message is displayed:

> Continuing with this load operation will delete the
> current Node/Station list. Do you want to continue?

Decide whether to continue. Answer **[yes]** and press **[Enter]**.

When you merge a node list into the Internet Advisor, duplicate names and addresses are not detected. If you add new names and addresses to that node list, the instrument checks for duplicate names and addresses.

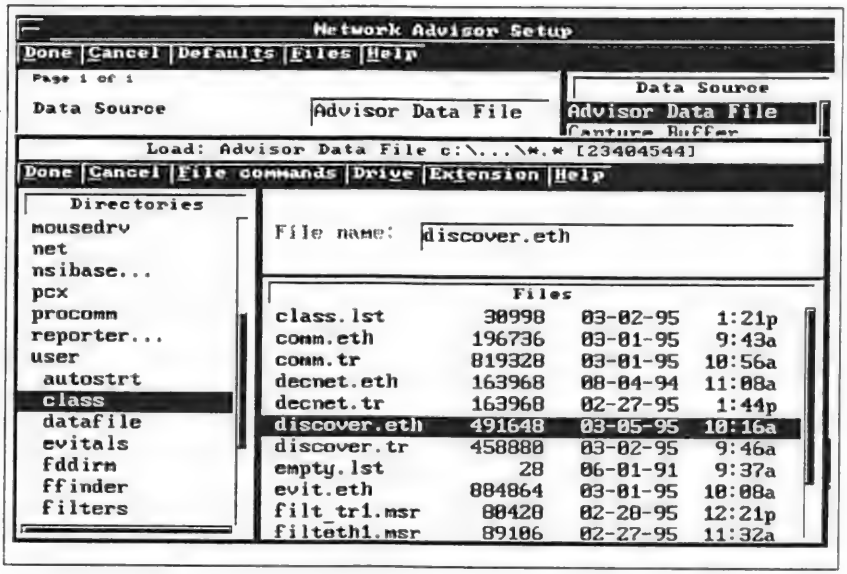
3. Press **[F4 | I]** to iconize the Node/Station List window.

Loading a Data File into the Capture Buffer

1. Click twice on the **SETUP** icon, or press **[F9]** to bring up the Setup window.

2. From the Data Source pane, type **[a]** for Advisor Data File and press **[Enter]**. You may see a message dialog box appear which asks if you would like to continue and destroy the capture buffer data; select **[yes]** and press **[Enter]**. The File Manager Data File Load window opens.

3. Notice the data file extensions are: (.eth) for Ethernet, (.trn) for Token-Ring and (.fdi) for FDDI. The default directory is ***c:\user\datafile***. In the Directories pane, change the directory to **[class]**. Tab to the Files pane and use the down arrow key to select the file **[discover.eth]** and select **[Done | Accept selection and exit]**. A dialog message box displays the frame numbers as they are downloaded into the capture buffer. Notice that the green status icon for the Data Source changes to Capture Buffer.



Loading an Advisor Data File

4. When the Advisor Data File has loaded, press **[F4 | I]** to iconize the Setup window.

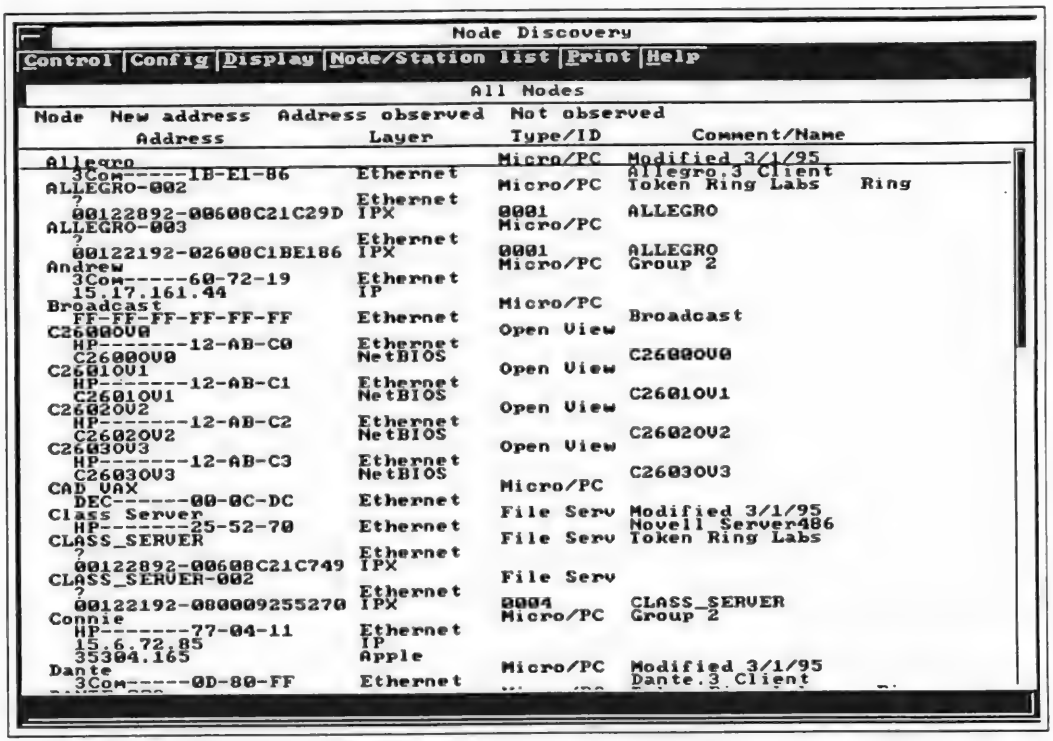
Note: The above process will be used to load Advisor Data Files in the following chapters.

View Network Node Discovery

With the node discovery capability, the Internet Advisor keeps track of which nodes are active and which are not. By monitoring all traffic and comparing it with a node list, the instrument tells you which nodes are observed, which are new, and which are inactive.

1. From the Measurements window, Network Discovery category, select **[Node Discovery]** and press **[Enter]**.

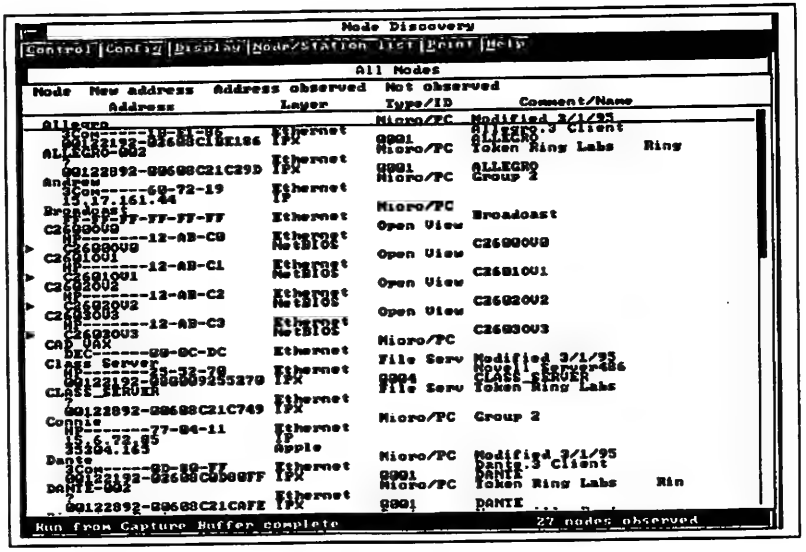
2. Press **[F4 | Z]** to zoom the Node Discovery window. From the menu bar, select **[Display | Display all known nodes]**. You see the existing node list from ***current.lst*** displayed in the Node Discovery window.



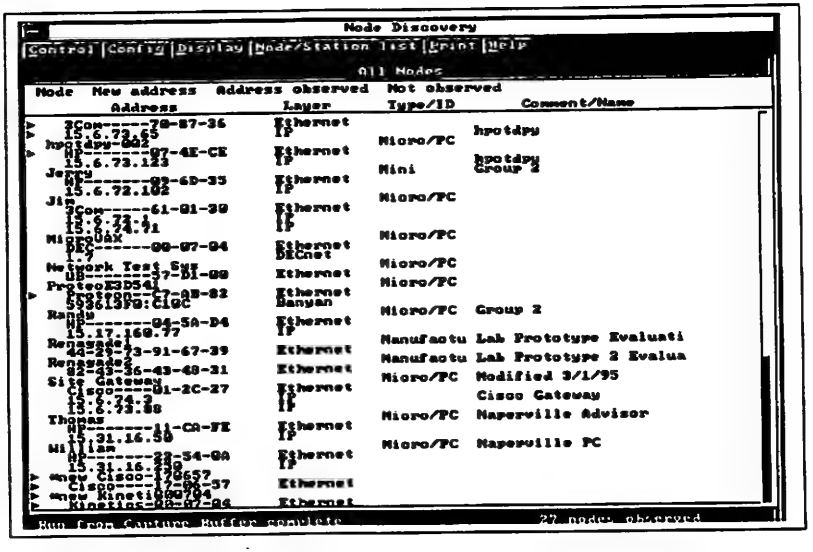
Node Discovery displaying nodes from the node list

Discover Additional Nodes

1. In the Node Discovery window, select **[Control | Run Measurement From Capture Buffer | All Frames]** from the menu bar. After three seconds, the Node List changes in several ways. Many of the nodes change from blue to green, indicating a known node that has transmitted frames on the network. The new nodes observed are displayed in red. Scroll down using the vertical scroll bar, or Next Page/Prev Page keys to view new entries.



New nodes discovered with Node Discovery



Additional nodes discovered with Node Discovery

When viewing nodes using Node Discovery you can select, **[Display]** from the menu bar, and display nodes in the following manner:

- Display all known nodes
- Display observed nodes only
- Display new nodes and mapping changes only
- Display new nodes only
- Display mapping changes but not new nodes

Information in the Node Discovery window is color-coded according to the line above the column headings.

- Black identifies the node name from the node list, a name extracted from a frame seen on the network, or a default name.
- Red identifies an address not listed in the current node list, but which has generated traffic on the network.
- Green identifies an address in the current node list that has generated traffic on the network.
- Blue identifies an address listed in the current node list that has not generated traffic on the network.
- Gray identifies a new name observed for a network address that has not yet generated any traffic. When traffic is observed from the address, the gray line changes to red.

Five main protocols are discovered by Node Discovery:

- IP
- Novell
- DECnet
- NetBIOS
- XNS

2. Review the context-sensitive help text for more detailed information. From the Node Discovery window, select **[Help | Node Discovery topics]** from the menu bar.

3. After reviewing the Help text, press **[F5]** to close the Help text window.

Merge the New Nodes

1. From the Node Discovery window, select **[Node/Station list | Merge selected records into Node/Station List]** and press **[Enter]**. This appends/merges the new node list entries into a "clone" of ***class.lst***, known as ***current.lst***, which is invisible to the file manager. Select **[Yes]** and press **[Enter]** when the merge process presents the following question:

> This action will add all addresses marked with a solid right arrow to your Node/Station list. It may require 1 second per address, or longer, with large lists. Do you want to do this?

2. Click on the **NODELST** icon, or press **[F11]** to open the Node/Station List window.

3. From the menu bar, select **[Files | Save Node/Station List]** to save the current node list which includes the newly discovered nodes/stations.

4. Enter the file name **[temp.lst]** to save the node list. Then, from the menu bar, select **[Done | Accept selection and exit]**.

5. Press **[F4 | I]** to iconize the Node/Station List window, and press **[F5]** to close the Node Discovery.

Create a Node List from Your Network

1. Click on the **NODELST** icon, or press **[F11]** to open the Node/Station List window. From the menu bar, select **[Files | Load Node/Station List | Replace Node/Station List]**.

2. Select the file **[c:\user\nodelist\empty.lst]** and from the menu bar, select **[Done | Accept selection and exit]**. Answer **[yes]** to the warning message and press **[Enter]**.

3. Press **[F4 | I]** to iconize the Node/Station List.

4. In the Measurements window, Network Discovery category, select **[Node Discovery]** and press **[Enter]**. From the menu bar, select **[Control | Run measurement from network]**. Node Discovery monitors frames seen on the network and displays new nodes.

5. After some nodes have been found, select **[Control | Switch to capture buffer]** from the menu bar . From the menu bar, select **[Node/Station List | Merge selected records into Node/Station List]**.

6. Press **[F5]** to close the Node Discovery measurement. Open the Node/Station List by clicking on the **NODELST** icon, or pressing **[F11]**. The discovered nodes are in the current list.

7. From the menu bar, select **[Files | Save Node/Station List]**. File Manager window opens to the default directory ***c:\user\nodelist***. Name your new node list and from the menu bar, select **[Done | Accept selection and exit]**.

8. Press **[F4 | I]** to iconize the Node/Station List.

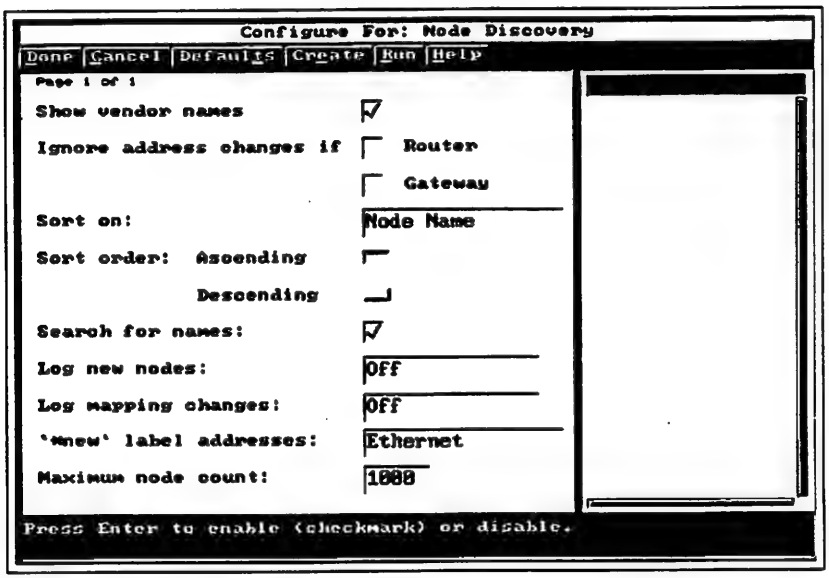
Node Discovery Configuration

You can control the display of Ethernet addresses, the sorting criteria for displayed node and address records, and the posting of events to the Event Log.

View Node Discovery Configuration Items

1. From the Measurements window, Network Discovery category, select **[Node Discovery]** and press **[Enter]**. From the menu bar, select **[Config | Configure Node Discovery]**.

If the Node Discovery measurement is still running when you open the Configuration window, some fields are grayed out; you can only view those current configuration item settings. Before changing those configuration items, you must stop the measurement.



Node Discovery configuration window

2. Examine the functions of Node Discovery configuration items in the following table.

Configure Item	Function	
Show vendor names	When enabled, addresses not present in the Node/Station List are displayed with the vendor name corresponding to the three most significant bytes of the Ethernet address. The three least significant bytes of the Ethernet address are displayed in hex. Vendor names can be added to the vendor dictionary by editing the file c:\analyzer\bundles\basic3\mfgdict.nls. When disabled, Ethernet addresses are displayed in hex.	
Ignore address changes if	When disabled, the Node Discovery measurement observes multiple higher level addresses for nodes that are routers or gateways. This means that all network addresses, of frames routed by this device are associated with this device's MAC address. When enabled, this prevents the Node Discovery Measurement from considering upper layer addresses to be address changes. To enable: 1. Check the Router box to ignore address changes for nodes that are router node type. 2. Check the Gateway box to ignore address changes for nodes that are gateway node type.	
Sort on	To change the order in which node name and address records are displayed in the Node Discovery window. The following sort criteria are available:	
	Node Name	Sorts on the record name in the node list. New node records are sorted (in the ascending sort) after all nodes in the node list. New nodes are given their Ethernet physical address as a default name.
	Node Type	Sorts on the Node Type attribute of the node. New node records receive a default Node Type of Micro/PC.
	Physical Address	Sorts on the Ethernet physical address.
	Physical ID	Sorts on the Cable ID attribute of the node list. New node records do not receive a Cable ID and therefore are first in the sort order.
	Physical Address Name	Sorts on the Address record name associated with the Ethernet physical address. New node records do not receive a physical name and therefore are first in the sort order.
Sort order	For all Sort On options, choosing Ascending results in a lowest-to-highest ordering. Choosing Descending results in a highest-to-lowest ordering.	

Search for names	When selected (a checkmark is displayed), the Discovery measurement looks at the contents of packets to find network names for IP, IPX, and NetBIOS addresses. These names are shown under the Name/Comment column in the Node Discovery measurement. If you create a node list from the Node Discovery measurement, these names are used as the node name for their corresponding address. When not selected, the Node Discovery measurement does not find names for the addresses it discovers. This may reduce the clutter of the display and speed up the packet processing, especially if your network has a large amount of traffic from name servers.	
Log new nodes	Lets you control the posting of new node events to the Event Log. A new node event occurs when an Ethernet address is observed that is not present in the Node/Station List. The following options are available:	
	Off	No event is posted. Recommended for the first run of Node Discovery.
	Normal Event	When a new node event occurs, an event is posted to the Event Log with the "normal" attribute. These events are green in the Event Log window.
	Warning Event	When a new node event occurs, an event is posted to the Event Log with the "warning" attribute. These events are yellow in the Event Log window.
	Alert Event	When a new node event occurs, an event is posted to the Event Log with the "alert" attribute. These events are red in the Event Log window.
Log mapping changes	Lets you control the posting of new address events to the Event Log. A mapping change event occurs when a protocol address is observed which is not present for the associated node entry. The following options are available:	
	Off	No event is posted.
	Normal Event	When a new address event occurs, an event is posted to the Event Log with the "normal" attribute. Normal events are green in the Event Log window.
	Warning Event	When a new address event occurs, an event is posted to the Event Log with the "warning" attribute. Warning events are yellow in the Event Log window.
	Alert Event	When a new address event occurs, an event is posted to the Event Log with the "alert" attribute. Alert events are red in the Event Log window.

*new label addresses	Determines how '*new' node names are displayed in the Node Discovery window. When you select and enter an address format from the choices in the list pane, a '*new' type node is displayed when an address is observed on the network, but there is no corresponding name available. For example: If the value of this field is IP, Ethernet, and if an IP address is found, the format for the '*new' address is *new 15.17.140.201. If an IP address cannot be found, the '*new' address is *new 000800A13223 for an Ethernet address.
Maximum node count	Determines how many nodes can be listed in the Node Discovery window. The current node list is automatically inserted in the Node Discovery window. The valid range of values for this field is from 100 to 8000.

4. From the menu bar select **[Done | Accept changes and exit]**. Press **[F5]** to close the Node Discovery window.

Addresses and Names Found by Node Discovery

Node Discovery finds all addresses on the local network. MAC addresses, as well as network layer addresses are found. The Node Discovery window shows new nodes discovered and nodes already entered in the node list.

Ethernet addresses (MAC or physical address) are reported when they are first observed in the source address field of a legal Ethernet frame. Addresses are also discovered for the following protocols:

- Internet Protocol (IP)
- Netware Internet Packet Exchange Protocol (IPX)
- DECnet
- IBM NetBIOS Protocol (NetBIOS)
- Xerox Network Services Internet Datagram Protocol (XNS)

Each discovered address is displayed on an indented address line. The associated node is determined by the Ethernet address of the frame carrying the traffic. Note that for the NetBIOS protocol, the address is considered to be the unique ASCII name representing a NetBIOS station. These names are usually transmitted only during the boot process of a NetBIOS node.

In addition to discovering addresses as nodes generate traffic on the network, the Internet Advisor for Ethernet associates names assigned by the system administrator to addresses when it can. Some protocols such as IP, IPX, and NetBIOS send packets from which names can be extracted. The Internet Advisor finds these "friendly" names and lets you use them instead of the default node names.

Load and Print the Node List

Before performing the following procedures, verify that the printer is configured correctly by referring to Chapter 1, page 11.

Load the Node List

1. Press **[F11]** key to open the Node/Station List. From the Node/Station List window, select **[Files | Load Node/Station List | Replace Node/Station List]** and press **[Enter]**.

2. From the Files pane, select the desired node list file that you'd like to print, then from the menu bar, select **[Done | Accept selection and exit]**.

Print the Node List

1. From the Measurements window, Network Discovery category, select **[Node Discovery]** and press **[Enter]**. The Node Discovery window opens and displays nodes in your node list.

2. From the menu bar, select **[Display | Display all known nodes]**. This ensures that all nodes in the node list are displayed.

3. From the menu bar, select **[Print | Print all displayed records]**. If you have a printer configured and connected, your node list will print. If your Internet Advisor is configured to print to file, then File Manager opens and you can copy the node list to an ASCII file on the hard drive or floppy disk.

4. Press **[F5]** to close Node Discovery.

Tune the Discovery Process Using Filters

You can tune the discovery process using filters.

For example:

- Filter #1—Server filter used for Node Discovery
  You can create a filter that captures frames to or from a file server. With this MAC "hardware" filter, you can build a node list of all nodes accessing the server.

- Filter #2—IP filter used for Node Discovery
  To discover nodes sourcing frames within a particular network subnet, for example, our network uses a 15.6.73.XX subnet. So, if you created a Basic IP Filter that specified frames sourced by node 15.6.73.XX, you would discover nodes using IP addresses 15.6.73.0 up to 15.6.73.255. This would help locate duplicate IP addresses.
- Filter #3—Router or Gateway Filter Used for Node Discovery
  To discover nodes sourcing frames from beyond the building's gateway or router, you can create a filter using the MAC address of the gateway or router and then use Node Discovery to identify any IP addresses of remote nodes.

Chapter Notes

Chapter Notes

Chapter 3 - Filters

Objective

The HP Internet Advisor captures every frame, regardless of the traffic level. This capability is absolutely necessary for accurate performance characterization, but sometimes you may want to focus the Internet Advisor on a particular problem. Use the Internet Advisor filtering capability to capture only the frames you need to see.

Filtering allows you to efficiently use the data capture buffer, as well as your own time by presenting only those frames that are related to the problem at hand. For example: If users are reporting a recurring problem with a print server, you could begin troubleshooting by capturing only the traffic to and from that server. Now all Internet Advisor measurements examine the frames that show you how the server is responding to print requests.

In this chapter, you will learn how to use existing hardware filters, create new custom filters, and activate the filters to allow for selective data capture.

Topics Covered

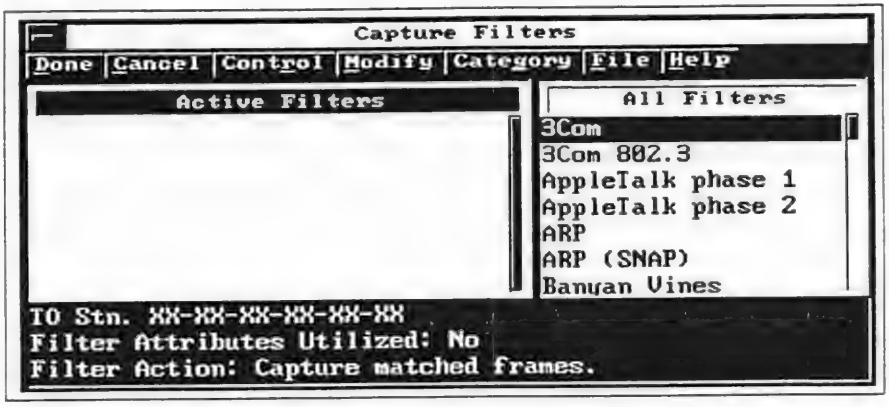
- Ethernet Capture Filter window
- Ethernet, IP, and IPX filter categories
- Creating an Ethernet MAC filter for a router
- Creating an IP filter for a nodal conversation
- Creating an IPX filter to examine a server
- Activating and deactivating filters
- Copy and delete custom filters

Preparation

- Internet Advisor for Ethernet should not have any measurements running.
- The Measurements window is properly sized and the categories are fully expanded.
- The Node List **c:\user\class\class.lst** should be loaded.

View the Capture Filters Window

The Capture Filters window allows you to select the data filters you want to use when capturing data. In the Capture Filters window, you select which frames are to be stored into the capture buffer.



Capture Filters window

- Status Icons - Of the eight graphic icons in the status panel in the lower right corner of the screen, the Filters icon is second from the left in the top row. When the icon is black, the filters are active. When the icon is white, the filters are inactive. Clicking on the icon will turn the filters on or off. Filters are defined in the Filters window.

The Internet Advisor for Ethernet Filters menu contains the following predefined Ethernet filter templates:

Ethernet Filter Types			
3Com	Basic Ethernet TCP	ICMP/IP (SNAP)	PING REQUEST
3Com 802.3	Basic Ethernet VIP	IGRP	RARP
Appletalk I	Broadcast Frames	IP (802.2)	RIP (Dest.)
Appletalk II	CLNP	IP (SNAP)	RIP (Source)
Arp	DEC LAT	NetBEUI	SNA path global
ARP (SNAP)	DEC LAVC	NetBIOS	SNA path individual
Banyan Vines	DEC LTM	Novell (FF-FF)	SNAP
Basic Ethernet	DEC MOP Dump/Load	Novell (SNAP)	SNMP 802.3
Basic Ethernet DDP	DEC MOP Remote	Novell RIP	SNMP (Ethernet)
Basic Ethernet DRP	DECnet IV	Novell SAP	Spanning Tree
Basic Ethernet IP	Error Frames	OSPF	TCP/IP (Ethernet)
Basic Ethernet IPX	FTP	PING	Telnet (Ethernet)
			UDP/IP (SNAP)
			XNS

Filter Data Using Addresses, Attributes, and Actions

You can filter data by assigning a MAC level, IP, or IPX (Novell) network level address for each filter, then combining these addresses to capture data in the following traffic modes:

- traffic from station 1
- traffic to station 1
- traffic to or from station 1
- traffic from station 1 to station 2
- traffic from station 2 to station 1
- traffic between station 1 to station 2
- from station 1 to multicast (Basic Ethernet Capture Filter only)

You can also filter frames by their attributes. For Ethernet, frame attributes include:

- good frames
- bad FCS frames
- runts
- jabbers
- dribbles

For additional filter capabilities, you can specify 48 bytes of data after the last filter field from the first page of the filter configuration.

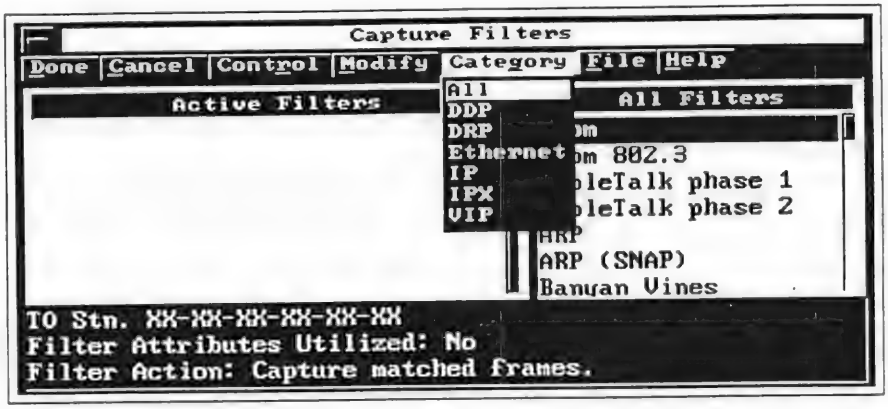
Example 1: In the Basic Ethernet filter the first page of the filter configuration window allows you to configure the Source and Destination addresses. On page two, byte 0 of the 48 bytes starts immediately after the Source Address in a Ethernet frame.

Example 2: In the Basic Ethernet IP filter the first page of the filter configuration window allows you to configure the network layer addresses and other network layer fields. On page two, byte 0 of the 48 bytes starts at layer 4, the transport layer - TCP.

Filter Categories

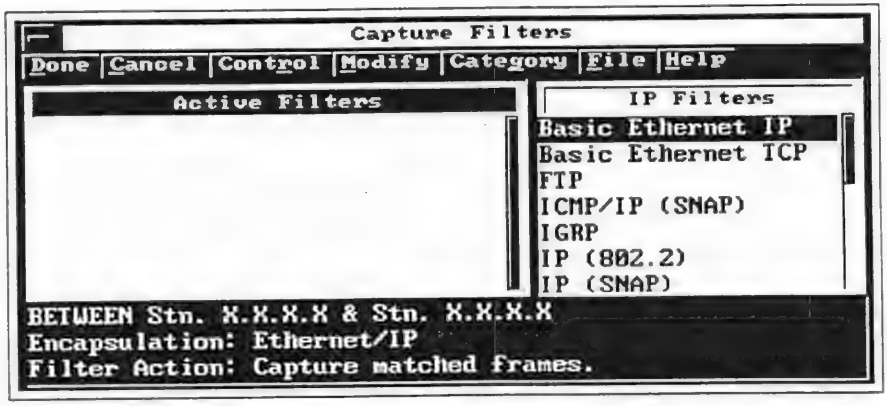
The following figure shows the filter categories available when you select the Category menu item.

1. Open the Filters window by pressing **[F12]** or clicking on the **FILTERS** icon. From the menu bar, select **[Category | All]** to view all the filters.



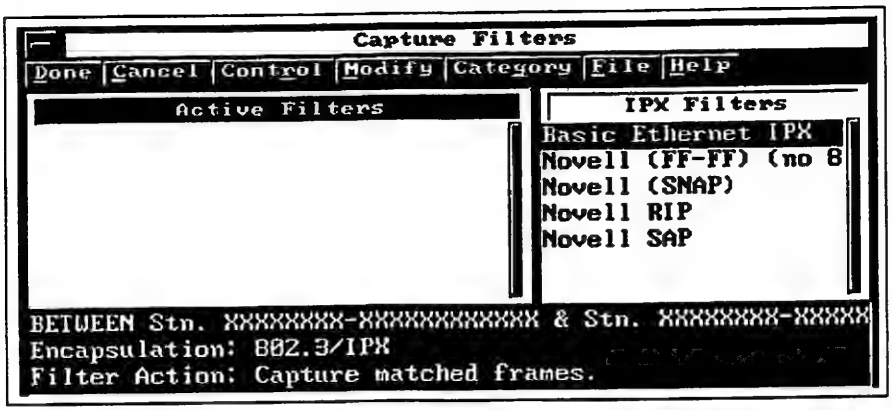
All Capture Filters displayed

2. From the menu bar, select **[Category | IP]** to view the IP filters.



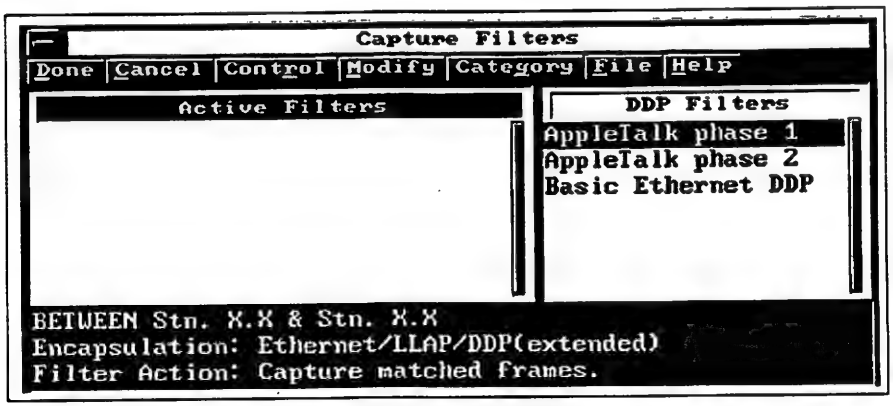
IP Capture Filters displayed

3. You can also select **[Category | IPX]** to view the IPX filters.



IPX Capture Filters displayed

4. You can also select **[Category | DDP]** to view the AppleTalk filters.



AppleTalk Capture Filters displayed

Create, Save and Name an Ethernet Router Filter

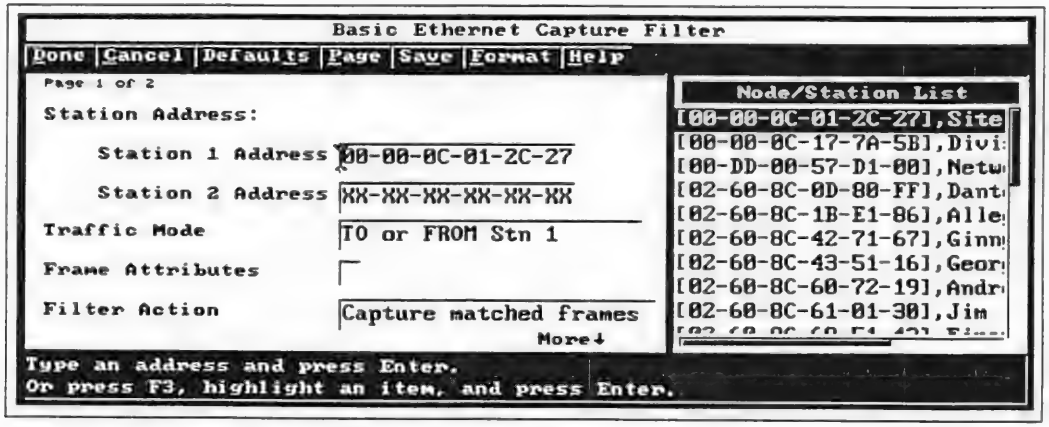
To create a new filter, you must first select an existing filter, then modify it, and save it using a new name.

1. Double click on the **FILTERS** icon at the bottom of the screen, or press **[F12]** to open the Capture Filters window.

2. From the menu bar, select **[Category | Ethernet]**. Cursor down to the **[Basic Ethernet]** and press **[Enter]**. A new window is displayed to allow you to modify the filter information.

3. From the Station 1 Address field, tab to the Node/Station List pane. The first node in the list should be "***site gateway***". Press **[Enter]** and notice that the MAC address 00-00-0C-01-2C-27 (Site Gateway's address) is automatically chosen from the Node/Station List.

4. Cursor down to the Traffic Mode and select **[TO or FROM Stn 1]** from the traffic mode pane. Cursor down to the Frame Attributes field and press **[Enter]** until the check mark disappears.



Basic Ethernet filter modified to capture data to and from the Site Gateway

5. From the menu bar, select **[Save | Save to new filter]**. Enter a new filter name, such as "Site Gateway", then press **[Enter]**. After saving your custom filter, restore the Basic Ethernet Filter to default values. From the menu bar, select **[Cancel | Cancel changes and exit]**. The Capture Filters window is displayed. Your new filter will be in the All Filters pane and the Basic Ethernet filter is still available for future use.

Create, Save and Name an Internet Protocol (IP) Conversation Filter

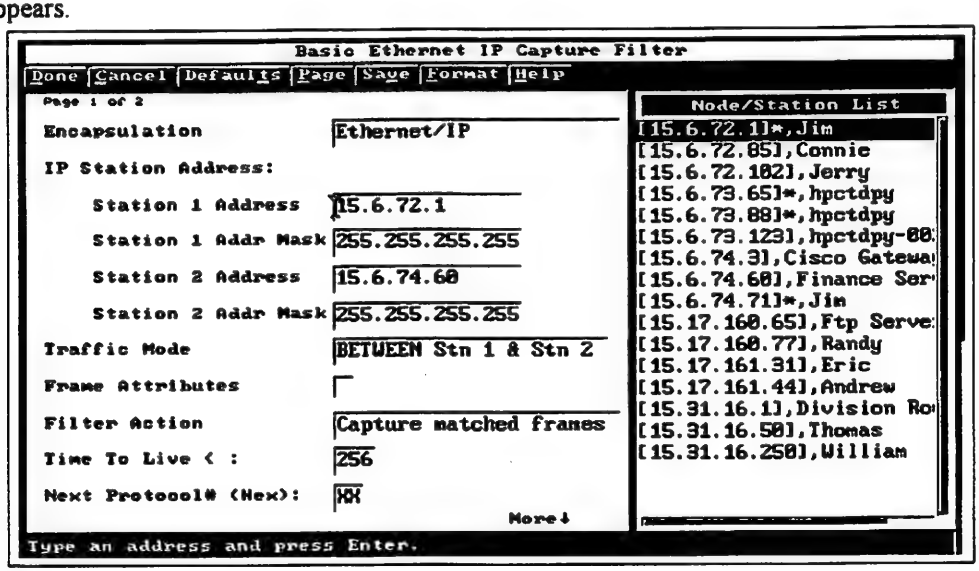
To create a new filter, you must first select an existing filter, then modify it, and save it using a new name.

1. Click on the **FILTERS** icon, or press **[F12]** to open the Capture Filters window.

2. From the menu bar, select **[Category | IP]**. Select the **[Basic Ethernet IP]** filter, then press **[Enter]**. A new window is displayed to allow you to modify the filter information.

3. Select the Station 1 Address field, tab to the Node/Station List pane, and type **[jim]** for Jim, then press **[Enter]**. Notice that the IP address 15.6.72.1 is automatically chosen from the Node/Station List. Now cursor to the Station 2 Address field, tab to the Node/Station List pane and type **[fi]** for Finance Server and press **[Enter]**. Its IP address is 15.6.74.60.

4. Cursor down to the Traffic Mode, and select **[Between Stn 1 & Stn 2]** from the traffic mode pane. Cursor down to the Frame Attributes field and press **[Enter]** until the check mark disappears.



Custom filter for traffic between Jim and Finance Server

5. From the menu bar, select **[Save | Save to new filter]**. Enter a new filter name, such as "Jim & Finance", then press **[Enter]**. After saving your custom filter, restore your Basic Ethernet IP Filter to default values. From the menu bar, select **[Cancel | Cancel changes and exit]**. The Capture Filters window is displayed. Your new filter will be in the All Filters pane and the Basic Ethernet IP Filter is still available for future use.

Note: Refer to page 9 for information pertaining to the Encapsulation field.

Create, Save, and Name an Internet Packet Exchange IPX Filter

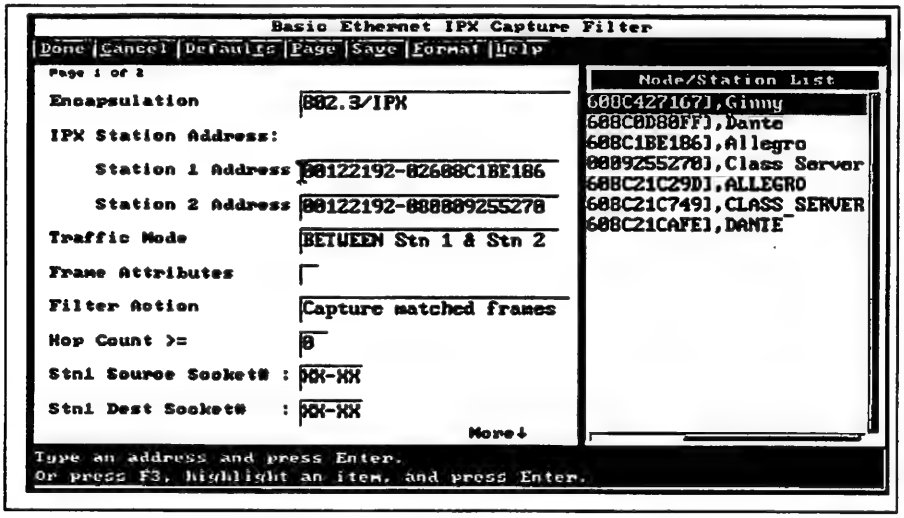
To create a new filter, you must first select an existing filter, then modify it, and save it using a new name.

1. Click on the **FILTERS** icon, or press **[F12]** to open the Capture Filters window.

2. From the menu bar, select **[Category | IPX]**. Select the **[Basic Ethernet IPX]** filter, then press **[Enter]**. A new window is displayed to allow you to modify the filter information.

3. Select the Station 1 Address field, then tab to the Node/Station List pane. Type **[al]** for Allegro and press **[Enter]**. Notice that the IPX address 00122192-02608C1BE186 is automatically chosen from the Node/Station List. Now cursor to the Station 2 Address field and tab to the Node/Station List pane and type **[cl]** for Class Server, and press **[Enter]**. Its address will be filled in.

4. Cursor down to Traffic Mode field and select **[Between Stn 1 & Stn 2]**. Cursor down to the Frame Attributes field and press **[Enter]** until the check mark disappears.



Custom IPX filter for traffic between Allegro and Class Server

5. From the menu bar, select **[Save | Save to new filter]**. Enter a filter name, such as "Allegro & Server", then press **[Enter]**. After saving your custom filter, restore your Basic Ethernet IPX Filter to default values. From the menu bar, select **[Cancel | Cancel changes and exit]**. The Capture Filters window is displayed. Your new filter will be in the All Filters pane and the Basic Ethernet IPX Filter is still available for future use.

Note: Refer to page 9 for information pertaining to the Encapsulation field.

Filter Encapsulation

Encapsulation lets you choose the lower layer protocol that encapsulates the IP or IPX protocol on your network. Try to select only the protocol encapsulation your network uses. This helps the Internet Advisor efficiently use the hardware needed for the filtering operation. If you do not know what encapsulation is used with either the IP or IPX packets on your network, select ***All,*** and the Internet Advisor will filter on all the protocols listed.

For the Basic Ethernet IP filter, you can select from the following encapsulation methods:

All
Ethernet/IP
802.3/802.2/IP
802.3/802.2/SNAP/IP

For the Basic Ethernet IPX filter, you can select from the following encapsulation methods:

All
Ethernet/IPX
802.3/IPX
802.3/802.2/IPX
802.3/802.2/SNAP/IPX

Activate or Deactivate a Filter

Activate a Filter

1. In the Capture Filters window, All Filters pane, cursor to the filter that you wish to activate and from the menu bar, select **[Control | Activate filter]**. You may activate several filters one at a time; they operate logically as an implied "OR" function. To exit, select **[Done | Accept changes and iconize]** from the menu bar.

Deactivate a Filter

1. In the Capture Filters window, Active Filters pane, cursor to the filter that you wish to deactivate, and from the menu bar, select **[Control | Deactivate filter]**. You may deactivate several filters one at a time. To exit select **[Done | Accept changes and iconize]** from the menu bar.

Filters can be easily activated or deactivated by simply clicking once on the filter icon field in the green status icons. Be sure that no measurements are running when activating or deactivating a filter.

Activating Multiple Filters

A maximum of 16 filters can be loaded and active simultaneously. When multiple filters are activated, the Internet Advisor captures frames that are the union of the activated filters.

For example:

- Two filters are created to **capture** matched frames.
  Filter #1 traffic mode is defined as "to or from station 1".
  Filter #2 traffic mode is defined as "to or from station 2".
  The filter action for both filters is set to capture matched frames.
  When these two filters are activated, the Internet Advisor captures only frames going to or coming from either node 1 or node 2.

- Two filters are created to **exclude** matched frames
  Filter #1 traffic mode is defined as "to or from station 1".
  Filter #2 traffic mode is defined as "to or from station 2".
  The filter action for both filters is set to exclude matched frames.
  When these two filters are activated, the Internet Advisor captures all frames, as well as the frames going to or coming from nodes 1 and 2, because each received frame is checked by all of the activated filters in parallel. While one filter may reject a frame, if another filter accepts the frame, it is saved in the capture buffer. For this reason, ***we recommend that only one filter be active when you are excluding matched frames.***

Restoring Default Filter Values

Restoring Defaults is used to restore default values to a pre-defined filter.

For example:

1. In the Capture Filters window, you choose to modify the Basic Ethernet capture filter.
2. You then insert two new physical station addresses for station 1 and station 2.
3. The next time you use the Basic Ethernet filter it would have two physical layer addresses instead of don't care characters. To restore the filter to its original settings, from the Capture Filters window, select **[Modify | Filter]**. From the filter window restore default values by selecting **[Defaults | Restore default values]** from the menu bar then selecting **[Done | Accept changes and exit]**. The filter will be restored to factory settings.

Copy and Delete Custom Filters

Copy Custom Filters

After creating a new filter, you may want to load it on another Internet Advisor for Ethernet. This can save you the time of re-creating the filter, and can ensure filters are identical on each Internet Advisor.

1. In the Capture Filter window, from the menu bar, select **[Category | All]**. Type the name of your filter. It will be automatically highlighted when a match is found.

2. From the menu bar, select **[File | Save user filter]**. The File Manager application will appear. You can save the filter to floppy by selecting, from File Managers menu bar, **[Drive | a:]**, and enter a valid MS-DOS(R) filename, then from the menu bar select **[Done | Accept selection and exit]**. This will copy your custom filter to a floppy disk.

Loading Your Filter on Another Internet Advisor

1. Open the Capture Filters window by pressing **[F12],** or double click on the **FILTERS** icon.

2. From the menu bar, select **[Category | All]**. From the menu bar, select **[File | Load user filter]**. File Manager will appear.

3. Insert the floppy disk containing the custom filter into the Internet Advisor's A drive. From the File Managers menu bar, select **[Drive | a:]**, select the appropriate file, then from the menu bar select **[Done | Accept selection and exit]**. Your custom filter will be loaded into the Internet Advisor filter list.

Note: Saving the filter to disk requires you to use a valid DOS filename. When you load the filter back into your Internet Advisor or another Internet Advisor, the original filter name is retained. The DOS filename is only required when copying the filter.

Delete Custom Filters

To delete a custom filter from the All Filters pane, follow the instructions below:

1. Open the Capture Filters window by pressing **[F12]** or double click on the **FILTERS** icon.

2. From the menu bar, select **[Category | All]**. Type the name of your filter until it is found.

3. When the filter is found and highlighted, select from the menu bar **[Control | Delete user filter]**. You will be asked if you really want to delete the filter.

Chapter Notes

Chapter 4 - Expert Advisor

Objective

The Expert Advisor provides an immediate graphical representation of your network's health. A single screen displays the results of Vital Signs, Protocol Statistics, Commentators and Node Discovery measurements, plus a continuous plot over time of network utilization and network health. Network health provides a quick, visual indicator of the general soundness of the LAN. Network health is measured by tracking warning and alert events (from Commentators) and errored frames (from Vital Signs) as they are observed on the network. A perfect network would have a health rating of 100 percent. However, running Expert Advisor on a real network, each error, warning and alert event reduces the network health percentage by a user-defined weighting factor. Normally, as network utilization rises, network health decreases. If network health decreases dramatically or drops during times of low utilization, your network probably has a significant problem.

Expert Advisor allows you to quickly identify potential network problems and drill down to the information needed to resolve those problems. If you were to run only one measurement in the Internet Advisor, this would be the one.

In this chapter, you will learn to configure the Expert Advisor and to use it to become more productive at troubleshooting and managing your network.

Topics Covered

- Expert Advisor overview
- Examine Expert Advisor screen and fields
- Drill down capability
- Examine drill down capability
- Using the Expert Advisor to troubleshoot a network problem
- Configuring Expert Advisor

Preparation

- Internet Advisor for Ethernet should not have any measurements running.
- The Measurements window is properly sized and the categories are fully expanded.
- The Node List **c:\user\class\class.lst** should be loaded.
- The Advisor Data File **c:\user\class\evit.eth** should be loaded into the capture buffer.

Expert Advisor Overview

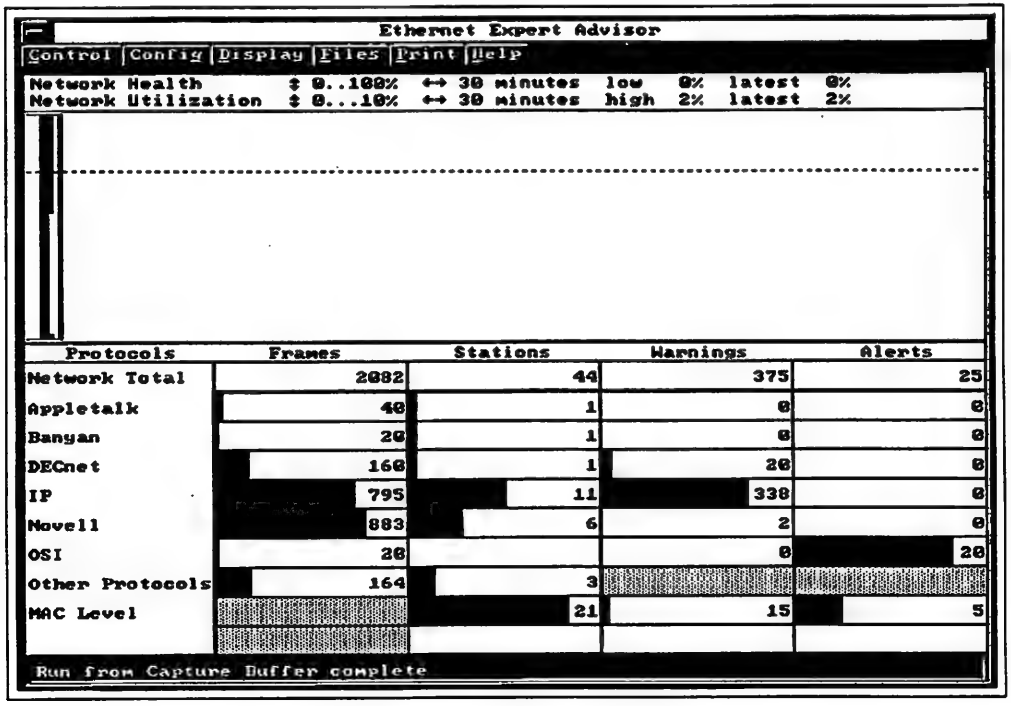
The Expert Advisor transforms data into meaningful information. It constantly monitors the traffic on your Ethernet, and reduces thousands of frames to a handful of significant events. It watches continuously for router misconfigurations, slow file transfers, inefficient window sizes, connection resets, and hundreds of other problems. And it does this for each protocol stack you have running, all in real time -- as events occur.

Event summaries tracked by the Expert Advisor are categorized by protocol stack, so you can quickly isolate problems to specific protocols.

1. From the Measurements window, Expert Advisor category, select **[Ethernet Expert Advisor]** and press **[Enter]**. Notice that the Expert Advisor window is displayed, and four icons appear at the bottom of the screen, indicating that an additional four measurements have started running.

2. From the menu bar, select **[Config | Configure Ethernet Expert Advisor]**. From the configuration window, select **[Defaults | Restore default values]**, and then select **[Done | Accept changes and exit]**.

2. From the Expert Advisor menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**. Expert Advisor may require approximately 30 seconds to re-play the capture buffer and display the results.



Ethernet Expert Advisor window

Examine Expert Advisor Screen and Fields

The Expert Advisor's screen updates every 10 seconds. Network Health and Network Utilization can be plotted over a 30 minute period. The *evit.eth* Advisor Data File contains information captured from monitoring a network for 1 minute, therefore, the Network Health and Network Utilization plots in the example on the previous page are short. Also, many frame errors occurred in the replayed data. Note that in the number of Warnings and Alerts versus the number of frames seen, approximately 20 percent of frames have errors. That is why the Network Health is rated zero. The algorithm for calculating Network Health is user configurable. Configuring the Expert Advisor will be covered later in this chapter.

The top portion of the Expert Advisor window shows both Network Health and Network Utilization. The bottom of the screen provides information on Protocols, Traffic, Stations, Warnings, and Alerts.

Most networks have several protocols operating concurrently. However, most network problems, other than physical layer problems, are related to a specific protocol. Even though each protocol can operate on your network simultaneously, each protocol operates as a separate logical network. Expert Advisor monitors the network and displays all the information by protocol to help you quickly understand and troubleshoot any problems. The table below describes each field in detail:

Expert Advisor field	Description
Protocol	Displays the protocols seen on the network. If a protocol field is grayed out, then no frames for that protocol stack have been observed.
Traffic: Displayed in Frames, Bytes, % Utilization, Bytes/sec, or Frames/sec.	Traffic can be displayed in frames, bytes, percent utilization, bytes a second, or frames a second. The default is frames, as in the previous example. The Network Total field displays total traffic observed from all protocols. The individual protocol fields have a traffic count corresponding to that protocol stack.
Stations	The Network Total field contains a count of all observed stations on the network under test. The individual protocol fields have a count of observed stations with network layer addresses corresponding to that protocol stack.
Warnings	The Network Total field contains a count of all Warning events observed on the network under test. The individual protocol fields have a count of all Warning events observed for that protocol stack.
Alerts	The Network Total field contains a count of all Alert events observed on the network test. The individual protocol fields have a count of all Alert events observed for that protocol stack.

Drill Down Capability

Expert Advisor's drill down capability allows you to access many of the measurements in the Internet Advisor. From the Expert Advisor, other measurements can be started simply by clicking on the Expert Advisor field of interest. Move the mouse pointer over the Expert Advisor fields, and watch it change from a pointer to a magnifying glass, which indicates that a drill down measurement is available.

If you don't have a mouse connected to the Internet Advisor, you can still drill down to additional measurements. From the Expert Advisor's window, the **[Display]** option is available from the menu bar. Select **[Display]**, and then you can select **[Utilization, Protocols, Traffic, Stations, Warnings, or Alerts]**.

The table below describes each drill down field in the Expert Advisor and the measurement started. The Warnings and Alerts fields have multiple drill down levels.

Expert Advisor field	Measurement started
Utilization	Starts Node Stats -- displays which nodes are talking on the network.
Protocol	Network Total field starts Protocol Stats configured to display all protocols by type and SAP. Individual Protocol fields, i.e., AppleTalk, IP, etc., start Protocol Stats configured to display only that protocol stack. If you drill down from IP Protocol, the Protocol Stats measurement will display FTP, WHO, ICMP, Telnet and any other IP types.
Traffic: Displayed as Frames, Bytes, % Utilization, Bytes/sec, or Frames/sec.	Network Total field starts Ethernet Vital Signs. Individual Frame fields, i.e., AppleTalk, IP, etc., start the individual Vital Sign measurement. If you drill down from IP frames, the TCP/IP Vital Signs will start.
Stations	Network Total field opens the Node Discovery measurement and displays all observed nodes. Individual Station fields, i.e., AppleTalk, IP, etc., open the Node Discovery measurement configured to display observed nodes with network layer addresses matching that protocol stack. If you drill down from IP Stations, Node Discovery will display only observed nodes that have IP layer addresses.

Warnings	Network Total field opens the Commentator measurement and displays a summary of warning events for all protocols. Individual Warning fields, i.e., AppleTalk, IP, etc., open the Commentator measurement and display a summary of warning events for that protocol stack. If you drill down from IP Warnings, Commentator will open and display, in summary, all IP Warning events. Additional drill down capabilities are available from the Commentator window. From the summary of warning events, further drill down can provide detailed Commentator information, and even further drill down can provide help text about the warning event or a decode display showing detailed information about the frame that caused the warning event.
Alerts	Network Total field opens the Commentator measurement and displays a summary of alert events for all protocols. Individual Alert fields, i.e., AppleTalk, IP, etc., open the Commentator measurement and displays a summary of alert events for that protocol stack. If you drill down from IP Alerts, Commentator will open and display, in summary, all IP Alert events. Additional drill down capabilities are available from the Commentator window. From the summary of alert events, further drill down can provide detailed Commentator information, and even further drill down can provide help text about the alert event or a decode display showing detailed information about the frame that caused the alert event.

Detailed information on each of these additional measurements can be found in other chapters of this manual. Refer to chapter 2 for information on Node/Station Discovery, chapter 5 for information on Node Stats or Protocol Stats, chapter 6 for information on the Vital Signs, and chapter 7 for information on the Commentators.

Examine Drill Down Capability to Other Measurements

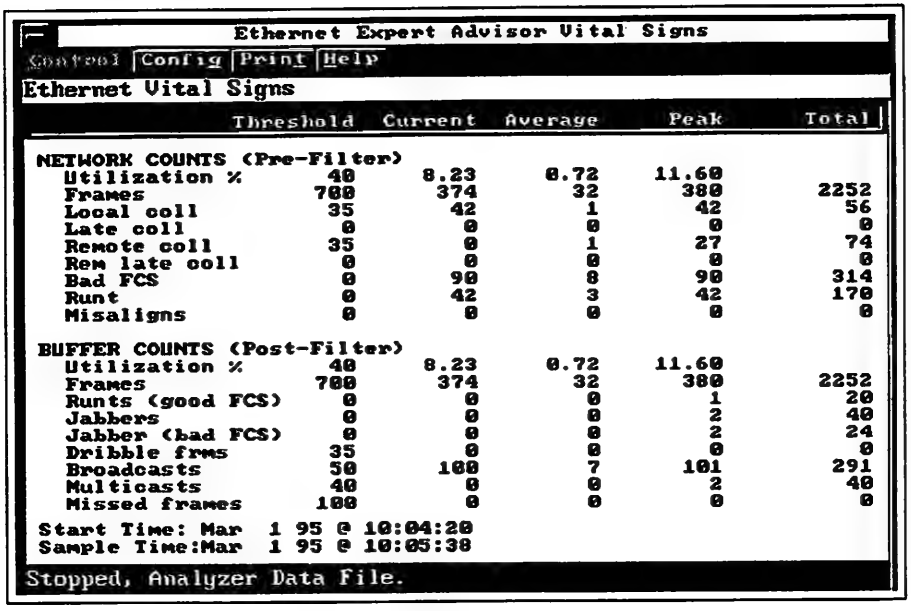
Your Internet Advisor should still have the Expert Advisor window open and the Advisor Data File ***evit.eth*** should have been replayed, as in the example on page 2 of this chapter.

In this section, several Internet Advisor measurements will be started using the drill down function in the Expert Advisor.

In the following example, you may use a mouse to point at a field and double click to drill down, or you may use the Expert Advisor screen menu bar by selecting **[Display]** and selecting the appropriate display option. In the following examples, measurements are performed using a mouse.

Review Network Total -- Frames

1. On the Expert Advisor screen, notice that Network Total for Frames is 2082. To review more detailed information about those frames, position the mouse pointer directly over the Network Total Frames count. Notice the mouse pointer changes to a magnifying glass. Double click the mouse so that the Ethernet Expert Advisor Vital Signs are displayed. Since the Expert Advisor replayed data from an Advisor Data File, the Vital Signs measurements automatically replay the same data.



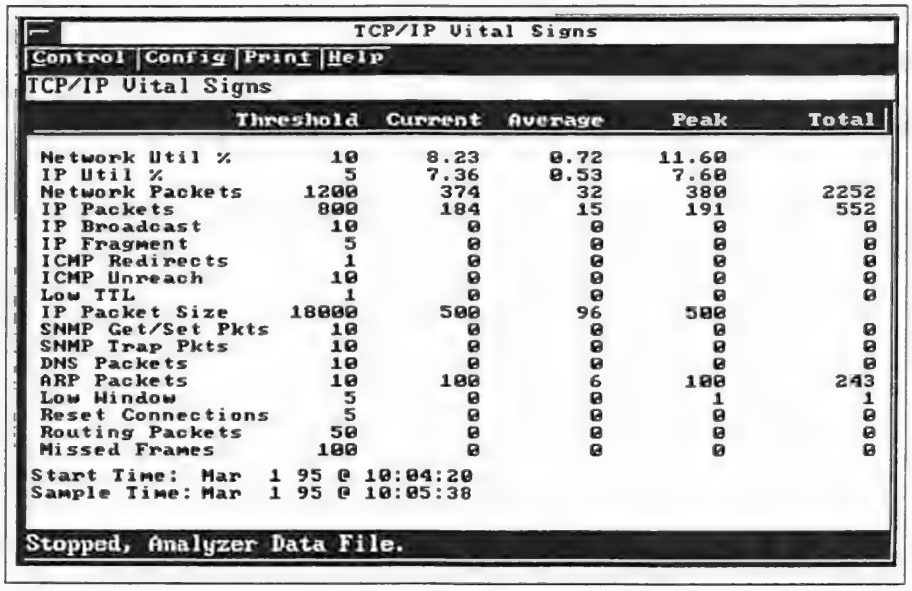
Ethernet Expert Advisor Vital Signs

The Vital Signs measurements give you detailed information about the traffic observed on the network. Physical layer problems can also be quickly identified with the Ethernet Vital Signs measurement. Context-sensitive help text is available in this, and all other measurements in the Internet Advisor for Ethernet. Review the help text for a detailed description of each field in the Vital Signs measurement.

2. Press **[F5]** to close, or iconize the Vital Signs measurement window.

Review IP -- Frames

3. On the Expert Advisor screen, the IP Frames count is 795. Position the mouse on the IP Frames count and double click. The TCP/IP Vital Signs automatically runs. These Vital Signs measurements provide you with detailed information about the TCP/IP frames observed on the network.



	Threshold	Current	Average	Peak	Total
Network Util %	10	8.23	0.72	11.60	
IP Util %	5	7.36	0.53	7.60	
Network Packets	1200	374	32	380	2252
IP Packets	800	184	15	191	552
IP Broadcast	10	0	0	0	0
IP Fragment	5	0	0	0	0
ICMP Redirects	1	0	0	0	0
ICMP Unreach	10	0	0	0	0
Low TTL	1	0	0	0	0
IP Packet Size	18000	500	96	500	
SNMP Get/Set Pkts	10	0	0	0	0
SNMP Trap Pkts	10	0	0	0	0
DNS Packets	10	0	0	0	0
ARP Packets	10	100	6	100	243
Low Window	5	0	0	1	1
Reset Connections	5	0	0	0	0
Routing Packets	50	0	0	0	0
Missed Frames	100	0	0	0	0

Start Time: Mar 1 95 @ 10:04:20
Sample Time: Mar 1 95 @ 10:05:38

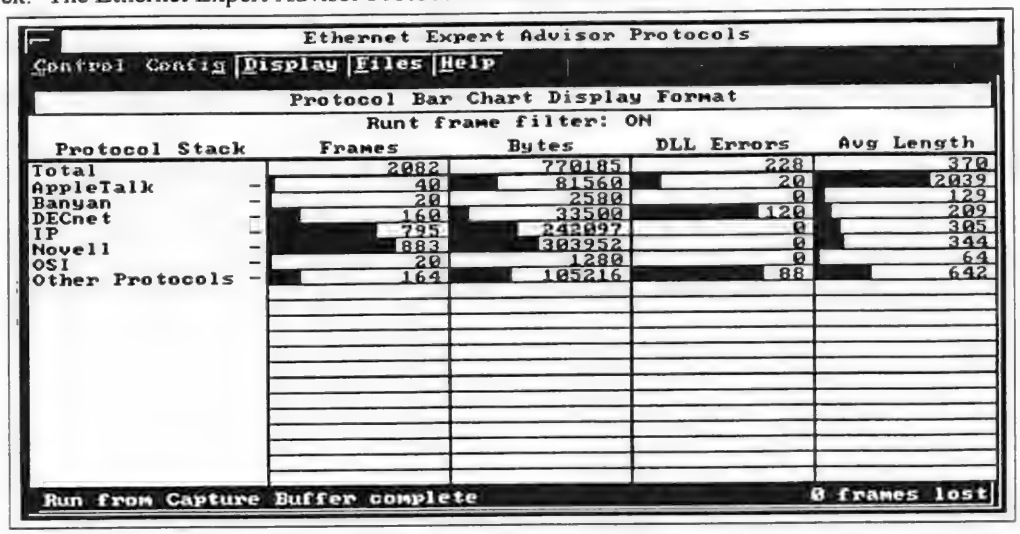
TCP/IP Vital Signs

If you selected DECnet Frames count and drilled down, the DECnet Vital Signs runs and provides you with detailed information about the DECnet traffic on your network. Your network may run other protocols, such as AppleTalk, Novell or Banyan. A Vital Signs measurement is available for each protocol stack.

4. Press **[F5]** to close the TCP/IP Vital Signs measurement.

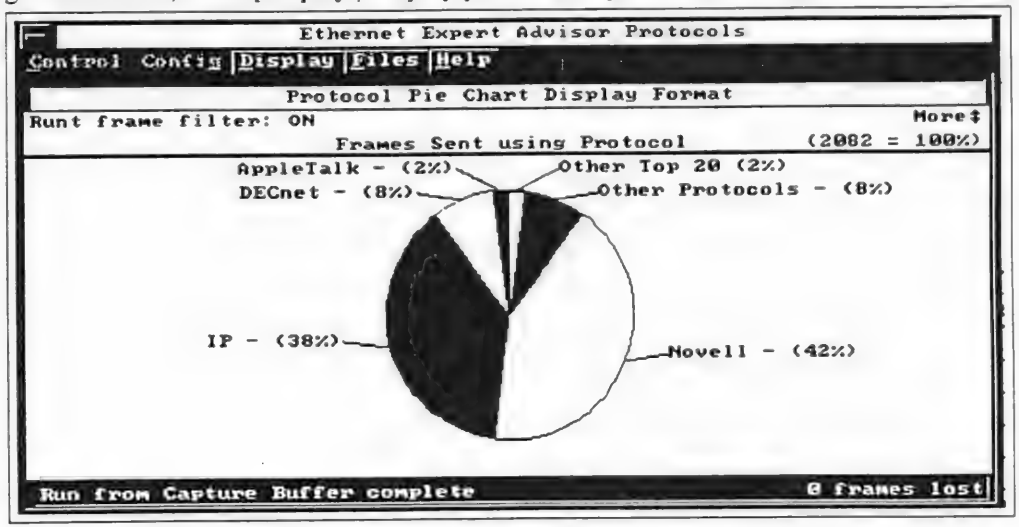
Review Network Total -- Protocols

5. Position the mouse pointer over the Network Total field in the Protocols category, and double click. The Ethernet Expert Advisor Protocols measurement runs.



Ethernet Expert Advisor Protocols

The Ethernet Expert Advisor Protocols provides detailed information about all the protocol stacks observed on your network, including frame length distribution. This information can be displayed in bar-chart or pie-chart format. To display in pie-chart format, or to display frame length distribution, select **[Display | Display protocols in pie chart format]** from the menu bar.

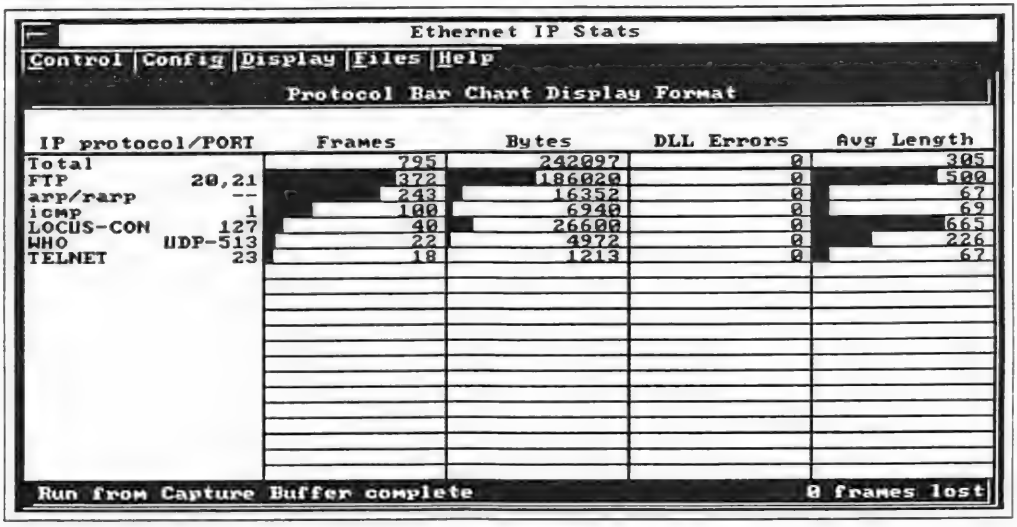


Ethernet Expert Advisor Protocols in pie-chart format

6. Press **[F5]** to close the Protocols window.

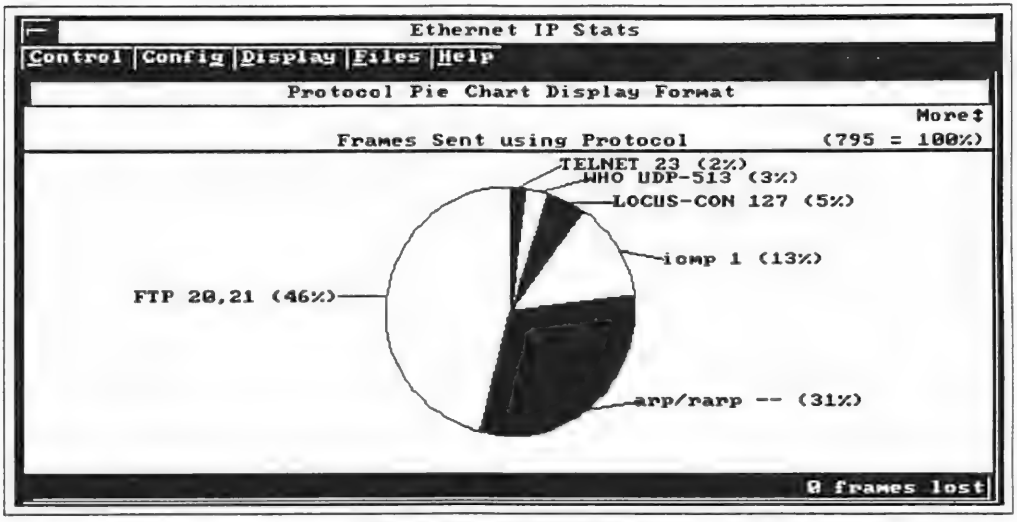
Review IP -- Protocols

7. Position the mouse pointer over the IP field in the Protocols category and double click. The Ethernet IP Stats measurement runs.



Ethernet IP Stats

Ethernet IP Stats provide detailed information about all the IP protocols observed on your network, including frame length distribution. This information can be displayed in bar-chart or pie-chart format. To display in pie-chart format, or to display frame length distribution, select **[Display | Display protocols in pie chart format]** from the menu bar.

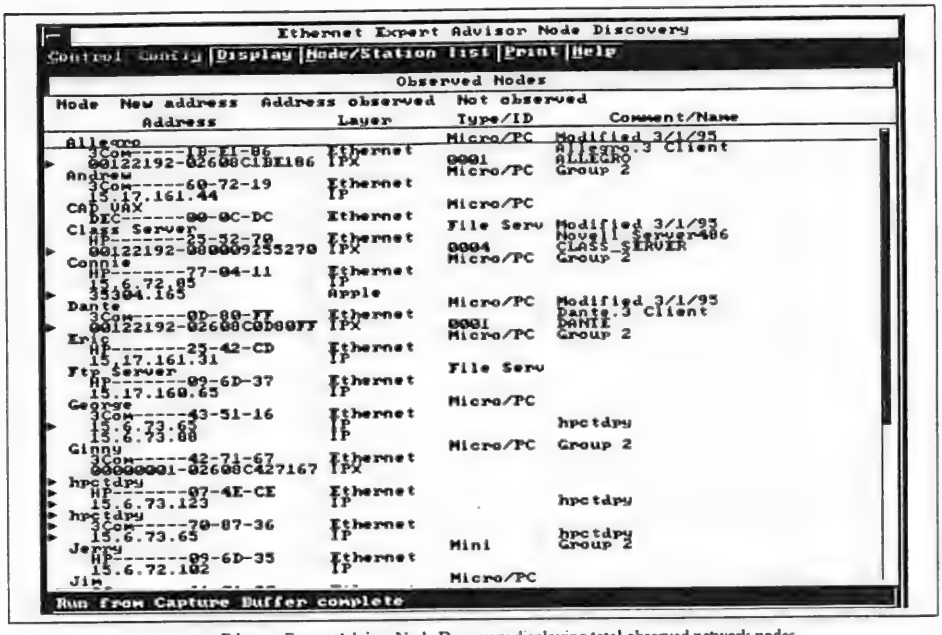


Ethernet IP Stats in pie-chart format

8. Press **[F5]** to close the Ethernet IP Stats measurement.

Review Network Total – Stations

9. On the Expert Advisor screen, the Network Total Stations count is 44. Position the mouse on the Network Total Stations count and double click. The Node Discovery measurement opens and displays all observed stations on the network.



Ethernet Expert Advisor Node Discovery displaying total observed network nodes

All the nodes observed on the network are displayed. Friendly names are observed and displayed along with physical layer addresses and network layer addresses.

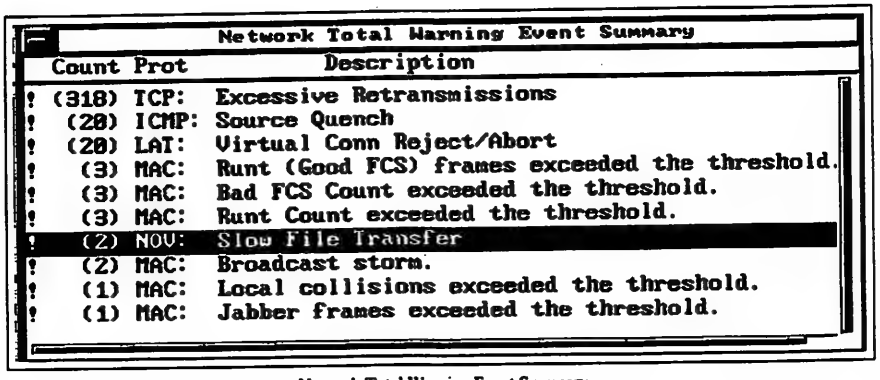
Refer to chapter 2 of this manual for detailed information about the Node Discovery measurement.

10. Press **[F5]** to close the Ethernet Expert Advisor Node Discovery measurement.

If you position the mouse on an individual protocol stack Stations count and double click, the Node Discovery measurement will open and display node information for any nodes observed, along with a network layer address that matches the protocol stack selected.

Review Network Total -- Warnings

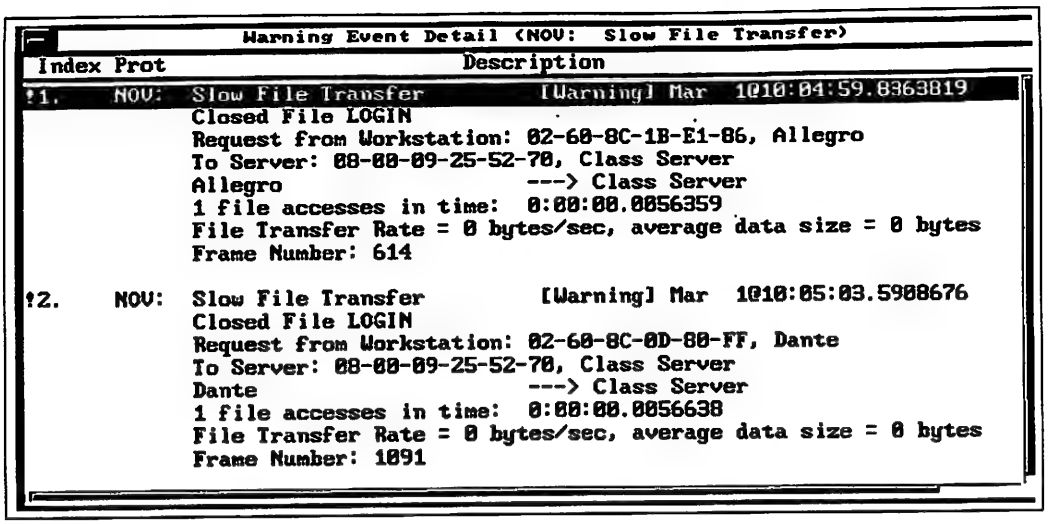
11. On the Expert Advisor screen, the Network Total Warnings count is 373. Position the mouse on the Network Total Warnings count and double click. The Network Total Warning Event Summary window opens, displaying all warnings the Commentator measurement observed. A description of the warning event is provided along with the total number of times that warning was observed.



Network Total Warning Event Summary

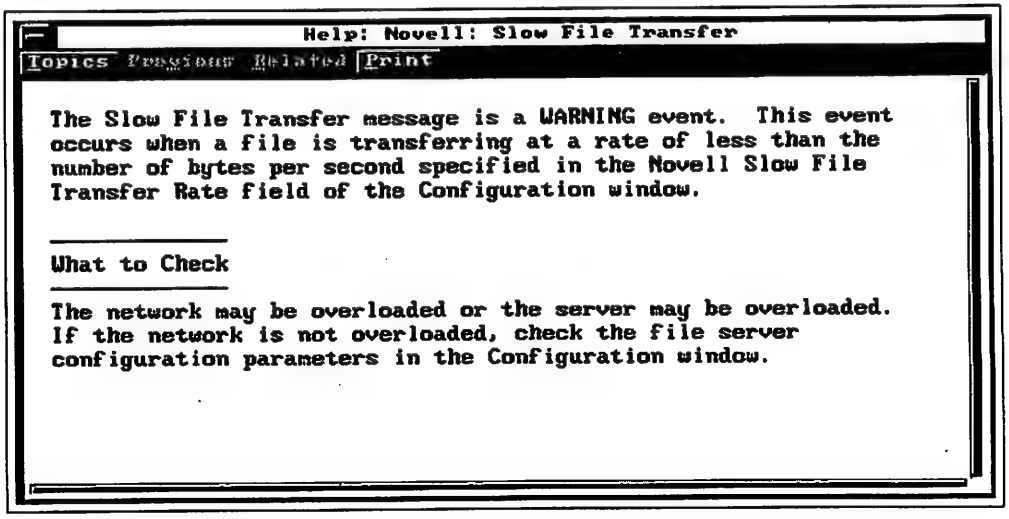
The summary window shows all the warning events observed, totaled by event. To get more detailed information about an event, position the mouse on the event and double click. Or, use the up or down arrow keys to highlight the event, and press enter.

12. Position the mouse on the "NOV: Slow File Transfer" event and double click. The Warning Event Detail window opens and displays each time a slow file transfer event occurred.



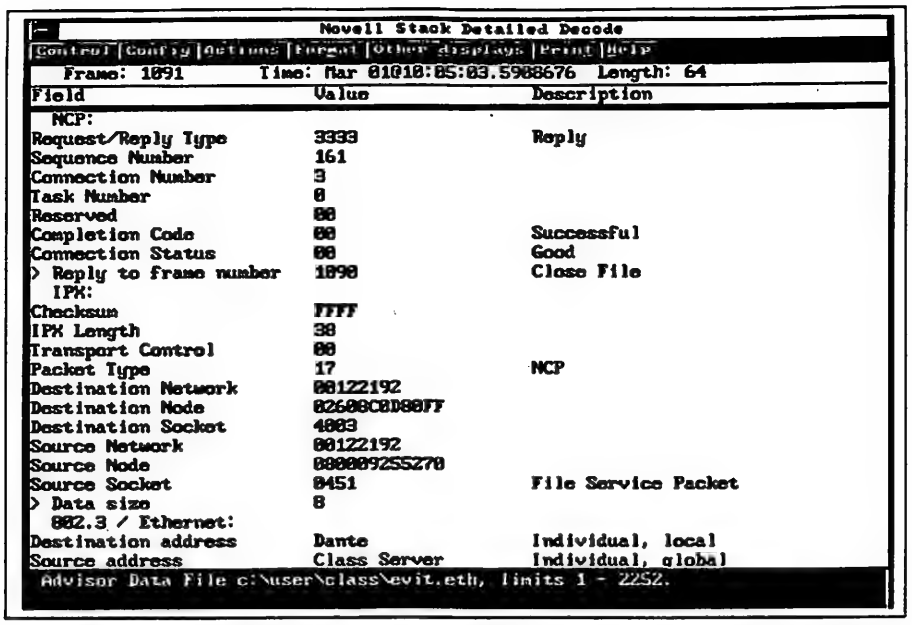
Warning Event Detail window

Notice that this window provides more detailed information about the slow file transfer. From this window, you can drill down to a decode of the specific frame in the capture buffer or drill down to the context-sensitive Help text that explains a slow file transfer. By positioning the mouse pointer over the description field (mouse pointer changes to a question mark) and double clicking, the context-sensitive Help text window will open and display information about the slow file transfer and possible causes of those frames.



Context-sensitive Help text for Novell Slow File Transfer

13. Press **[F5]** to close the Help text window. Position the mouse pointer over any other part of the detailed event and double click; a decode window opens and displays the last frame of the file transfer.



Novell Stack Detailed Decode displaying the Novell Close File frame

14. Press **[F5]** to close all open windows until the Expert Advisor is the only open window.

The Network Totals Warning window provides information about all the Warning events observed on the network. Selecting the Warnings by protocol stack opens the Warnings Event Summary for that specific protocol stack.

15. From the Expert Advisor window, position the mouse pointer on the MAC Level Warnings and double click. The MAC Level Warning Event Summary window opens and displays only MAC level events. By filtering the displayed data to show only the protocol stack selected, you can quickly identify problems in that protocol stack and take corrective action.

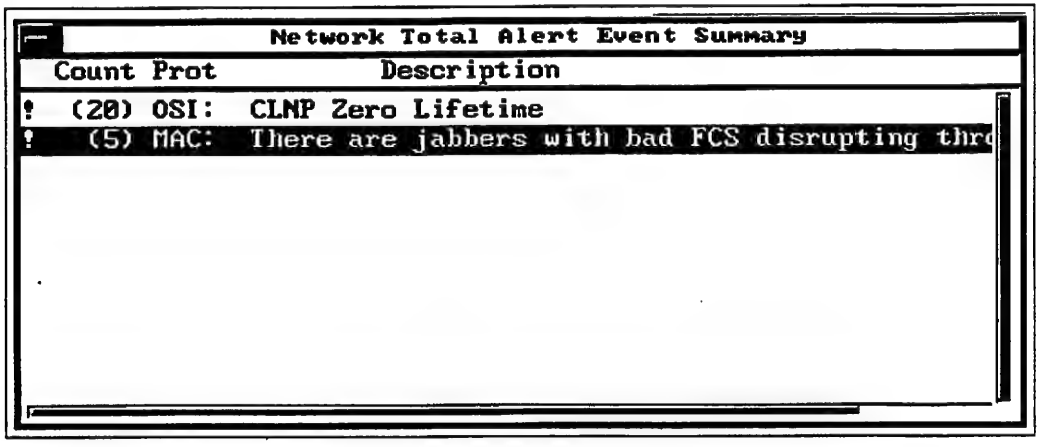
15. Press **[F5]** to close the MAC Level Warning Event Summary window.

Using the Expert Advisor to Troubleshoot a Network Problem

The Expert Advisor window provides information about the overall health of the network. After replaying the ***evit.eth*** data file and reviewing data presented in the Expert Advisor window and other drill down windows, you should have a thorough understanding of what is happening on your network.

The network under test (our evit.eth file) shows very poor Network Health. Although utilization is low, only averaging two percent, the Network Health is rated at zero. This is because approximately 20 percent of the frames on the network contain errors. The best method for correcting this problem is to start troubleshooting the most serious problem. In the Expert Advisor window, the Network Total Alerts field shows 25 alert events. 20 are OSI events, and 5 are categorized as MAC Level events. Your troubleshooting approach should be to review the most serious problems, the alert events, to understand them, and finally to take corrective action to eliminate them from the network.

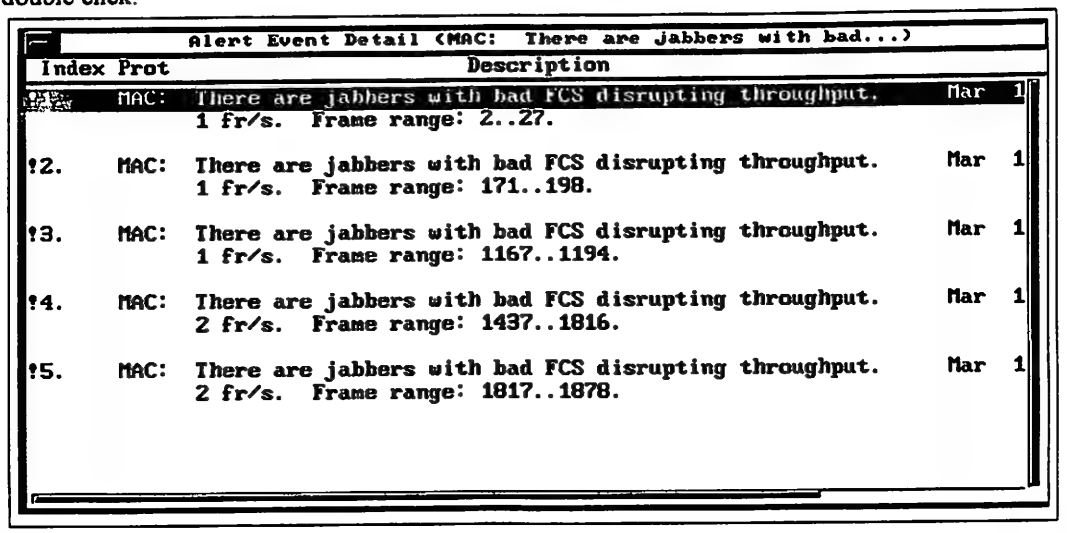
1. From the Expert Advisor window, position the mouse pointer on the Network Total Alerts field and double click.



Network Total Alert Event Summary window

The summary window provides information about 20 OSI CLNP Zero Lifetime events and 5 MAC jabber events. Two problems have been identified. MAC, or physical layer problems should be investigated first. Their impact on network performance is far reaching. How can you understand this MAC layer problem and identify who or what is causing it?

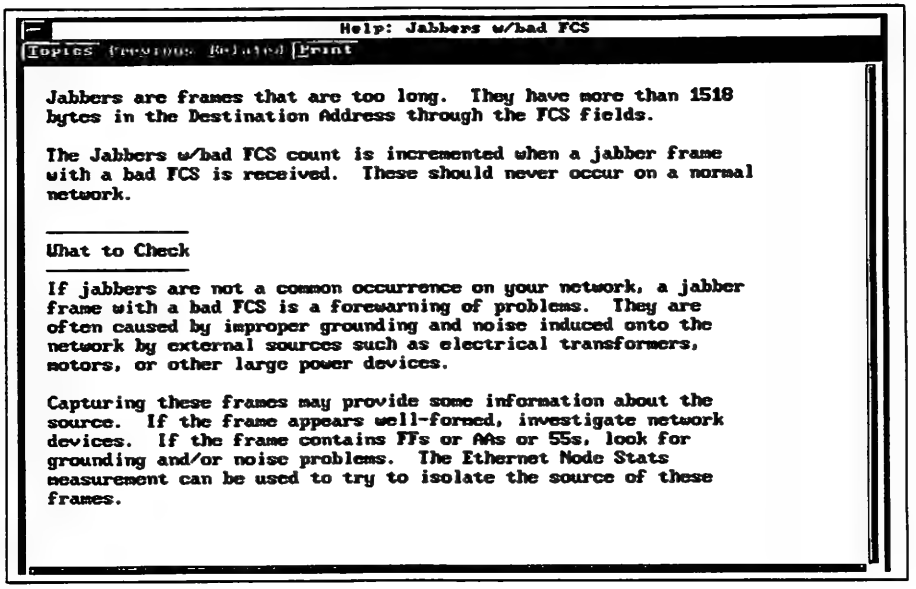
2. Position the mouse pointer on the description line for jabbers in the summary window and double click.



Alert Event Detail window displaying information about jabbers in more detail

Notice that in the first description line of the example above, a jabber occurred in the frame range 2 to 27.

3. Review the context-sensitive Help text to understand jabbers. Position the mouse pointer on the first description line "There are jabbers with bad FCS disrupting throughput." The mouse pointer will change to a "?". Double click.

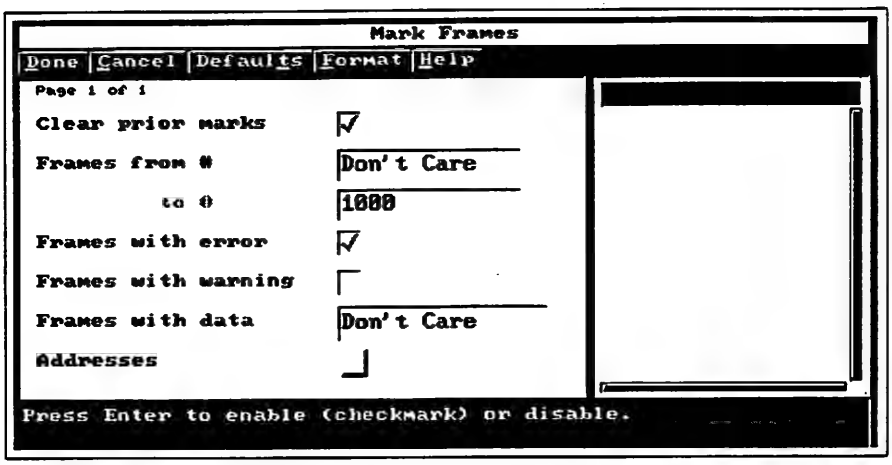


Context-sensitive Help text for Jabbers w/bad FCS

4. Press **[F5]** to close the Help text window.

5. To investigate the problem in more detail, position the mouse pointer on the frame range description line "1 fr/s. Frame range: 2..27." and double click. The last frame in the frame range is displayed, frame 27. The decode opened and displayed is the 802.3/Ethernet Detailed Decode, which displays data related to the MAC layer.

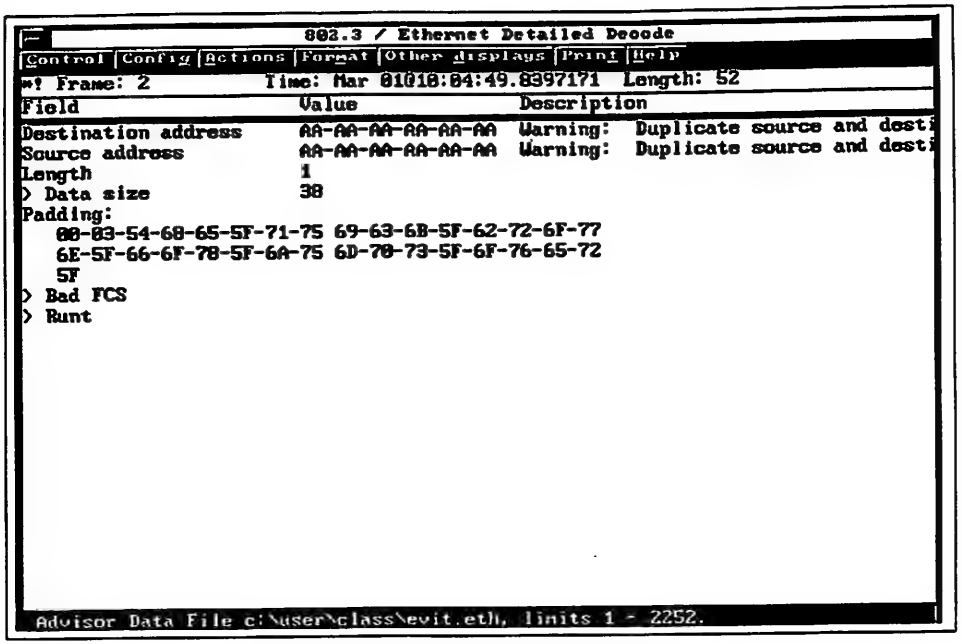
6. Press **[F4 | Z]** to zoom the decode window. From the menu bar, select **[Actions | Mark | Frames]**.



Mark Frames window

7. Configure your Mark Frames window with the same values in the example above. Then, from the menu bar select **[Done | Accept changes and exit]**.

8. From the menu bar, select **[Actions | Display | Marked frames]**. Only errored frames will be displayed. Press the **[Home]** key to display the first marked frame.



802.3 / Ethernet Detailed Decode displaying first marked frame

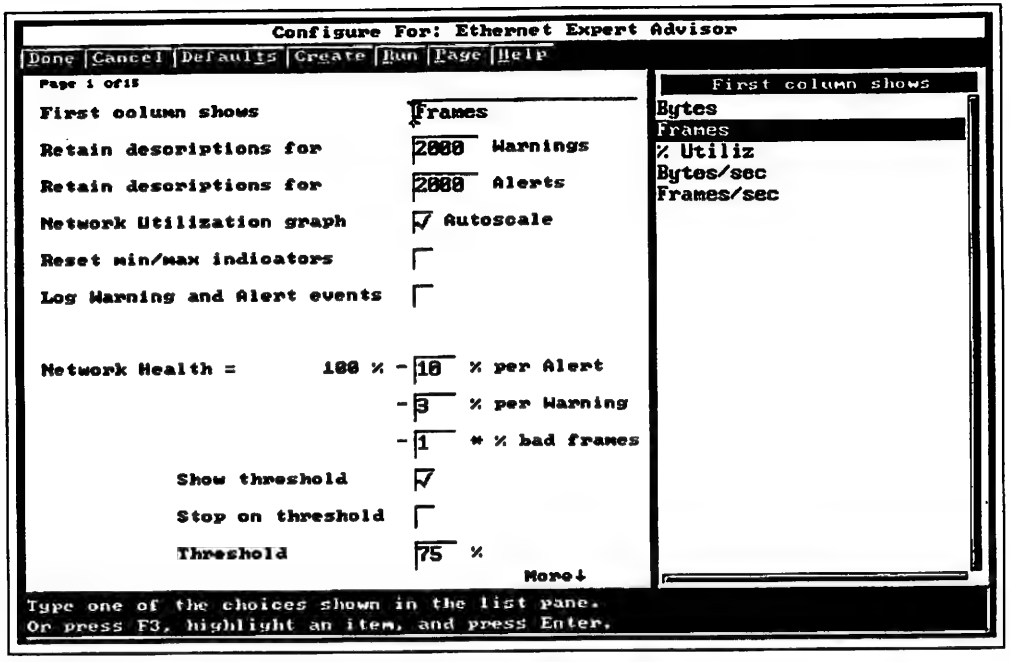
In the example above, frame number 2 is a collision fragment. The frame has a bad FCS, and is a runt frame. The source and destination addresses are AA-AA-AA-AA-AA-AA which indicates a jam signal.

9. Use the down arrow key to review the errored frames. Frames 9, 10, and 11 are jabber frames. From the decode of these three frames, you see that two nodes are sending those jabber frames, source addresses Synoptics-DE-ED-E0 and 3Com-92-04-03. Those NIC cards, or cabling, should be replaced to eliminate this problem.

10. Press **[F5]** to close each window until you return to the Expert Advisor window.

Configure the Expert Advisor

1. From the menu bar, select **[Config | Configure Ethernet Expert Advisor]**. From the menu bar, select **[Defaults | Restore default values]**.



Expert Advisor main configuration window

The Expert Advisor Configuration window lets you customize the Expert Advisor by configuring fields that control such parameters as:

- Information shown in the first column of the Ethernet Expert Advisor window.
- Number of Warnings and Alerts to be kept; whether to reset the high and low indicators in the Expert Advisor window.
- Whether the Network Utilization graph is autoscaled within the network utilization range, or whether it stays scaled at 100 percent.
- Whether Warning and Alert events are posted to the Internet Advisor's Event Log.
- How Network Health is calculated.
- Whether a user-defined threshold is displayed in the Network Health graph, and whether all running measurements are stopped if this threshold is exceeded

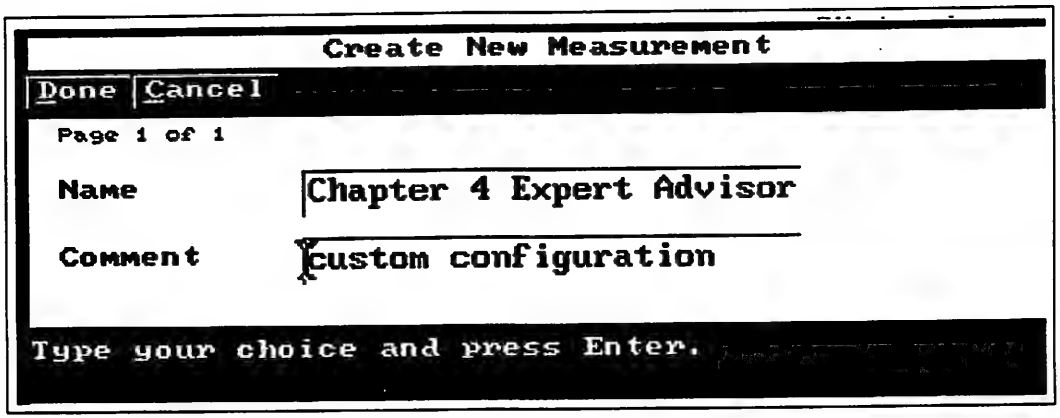
The Ethernet Expert Advisor Configuration window also lets you configure parameters for Commentators, Vital Signs, and Node Discovery. Refer to chapter 2 for configuring Node Discovery, chapter 6 for Vital Signs configuration, and chapter 7 for configuration information on Commentators.

Protocol Statistics have no configurable parameters in the Expert Advisor. Context-sensitive help text is available in the configuration windows. From the Configuration window menu bar, select **[Help | Configuration topics]** to learn more about configuring individual fields within the configuration windows. Select **[Done | Exit]** from the help text menu bar to close the window.

Create Additional Copies of the Expert Advisor

You can create and save multiple Expert Advisor measurements, which allows you the flexibility to configure the Expert Advisor for certain networks or network conditions. You can use these different configurations when you want to use the Expert Advisor on a different network.

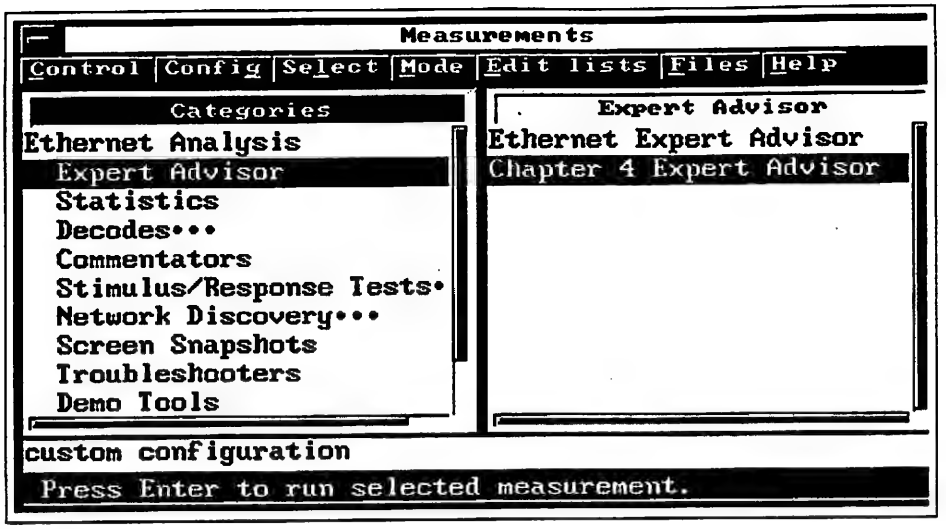
1. From the configuration window menu bar, select **[Create | Create new measurement]**. Enter any name and a comment field. For this example, use **[Chapter 4 Expert Advisor]** and **[custom configuration]** for the comment field.



Create New Measurement window within Configuration window

2. From the configuration window, select **[Done | Accept changes and exit]**. Then press **[F5]** to close the Expert Advisor window.

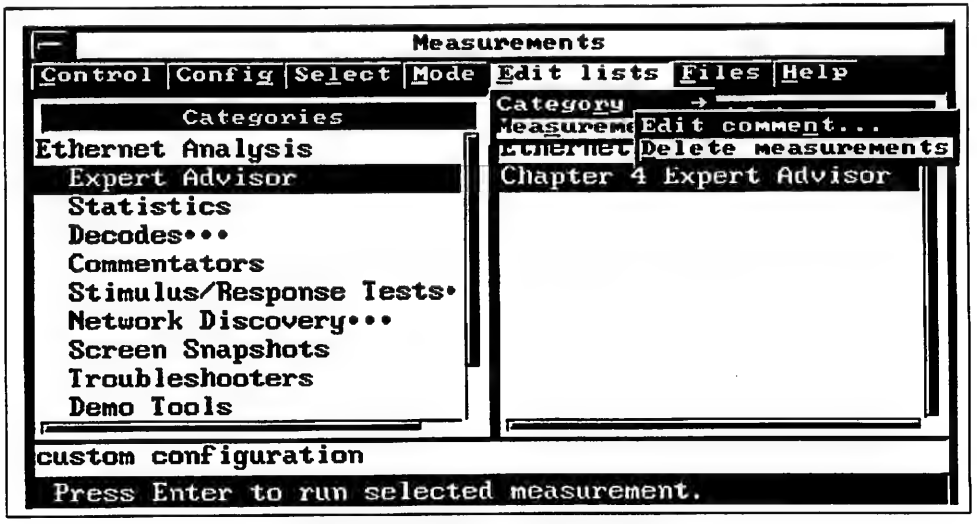
The Measurement window appears with the new "Chapter 4 Expert Advisor" measurement in the Expert Advisor category.



New Chapter 4 Expert Advisor measurement available in Measurements window

Chapter 4 Expert Advisor can be opened and configured to fit your particular testing needs, especially in the Network Health calculations.

4. To remove Chapter 4 Expert Advisor from the Measurement window, select **[Chapter 4 Expert Advisor]**, then from the Measurements window menu bar select **[Edit lists | Measurement | Delete measurement]**. A warning message will appear indicating you are deleting a measurement. Check whether you are deleting the proper one, and select **[yes]** and press **[Enter]**. Chapter 4 Expert Advisor is removed from the Expert Advisor category.



Removing a measurement from the Measurements window

Chapter Notes

Chapter Notes

Chapter 5 - Statistics

Objective

Network management requires an in-depth understanding of network behavior, and to meet this requirement you need a comprehensive set of analysis tools. The Internet Advisor for Ethernet has several powerful statistical measurements available to help you proactively manage and troubleshoot your network.

In this chapter you will learn about statistical measurements, how to configure them, and how to use them effectively.

Topics Covered

- Statistical Category overview
- Summary Statistics
- Node Statistics
- Protocol Statistics
- Connection Statistics
- Top Talkers
- Top Error Sources

Preparation

- Internet Advisor for Ethernet should not have any measurements running.
- The Measurements window is properly sized and the categories are fully expanded.
- The Node List **c:\user\class\class.lst** should be loaded.
- The Advisor Data File **c:\user\class\stats.eth** must be loaded into the capture buffer.

View the Statistics Categories

In the Measurements window, Statistics category, the following statistical measurements are available:

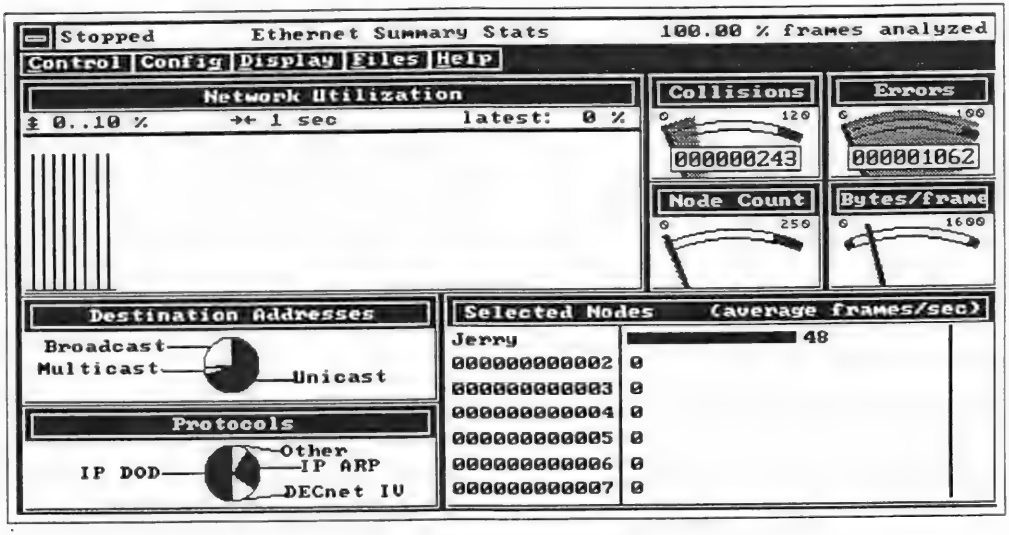
Ethernet Statistics	Summary of the Measurements
Summary Stats	Provides a summary of the activity on an Ethernet network, including network utilization, collisions, errors, node count, bytes/frame, destination addresses, selected nodes, and protocols.
Node Stats	Displays statistical information for up to 20 nodes. The following can be displayed for each node: volume of traffic in bytes or frames, type of traffic, broadcast or multicast, and number of errors.
Protocol Stats	Displays the types of protocols being used on your network. Frame length distribution by protocol is also available.
Connection Stats	Keeps track of conversation pairs by MAC address, or network address (IP, Novell IPX, DECnet, AppleTalk, Banyan or OSI). Using the Connection Statistics measurement, you can track errors and bandwidth utilization (by frames or by kbytes) by connection pair, and display the results in either bar-chart or pie-chart format.
IP Subnet Connection Stats	Same as Connection Stats measurement except this measurement keeps track of conversation pairs by IP Subnet address.
Top Talkers	Displays a list of up to 50 nodes that have generated the most frames since the measurement was started. Traffic volume in frames and bytes is displayed for each node.
Top Error Sources	Displays a list of up to 50 nodes that have generated the most error frames since the measurement was started. For each node, the number of total errors and the types of errors are reported.
Ethernet Vital Signs	Shows important information about an Ethernet network's performance, such as the number of collisions occurring on the network, and what percentage of the network's capacity is being used (utilization). Vital Signs also indicates the presence of potentially serious errors on your network; detects these errors by correlating the occurrence of collisions, errors, and good frames on an Ethernet network; and infers possible causes of the problems using the combination of errors in each frame.
Novell, TCP/IP, DECnet, AppleTalk, OSI, and Banyan Vital Signs	These measurements are covered in detail in chapter 6.

Run Summary Statistics

1. From the Measurements window, Statistics category, select **[Ethernet Summary Stats]** and press **[Enter]**.

2. From the menu bar, select **[Config | Configure Selected Nodes]**. Click on the Node 1 address field, or use the down arrow key until the Node 1 address field is highlighted. Tab to the Node/Station List pane and type **[Je]** for node Jerry. Press **[Enter]** and Jerry will be selected as the Node 1 address. From the menu bar select **[Done | Accept changes and exit]**.

3. From the Ethernet Summary Stats menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**.



Ethernet Summary Stats window

Drill Down Capability

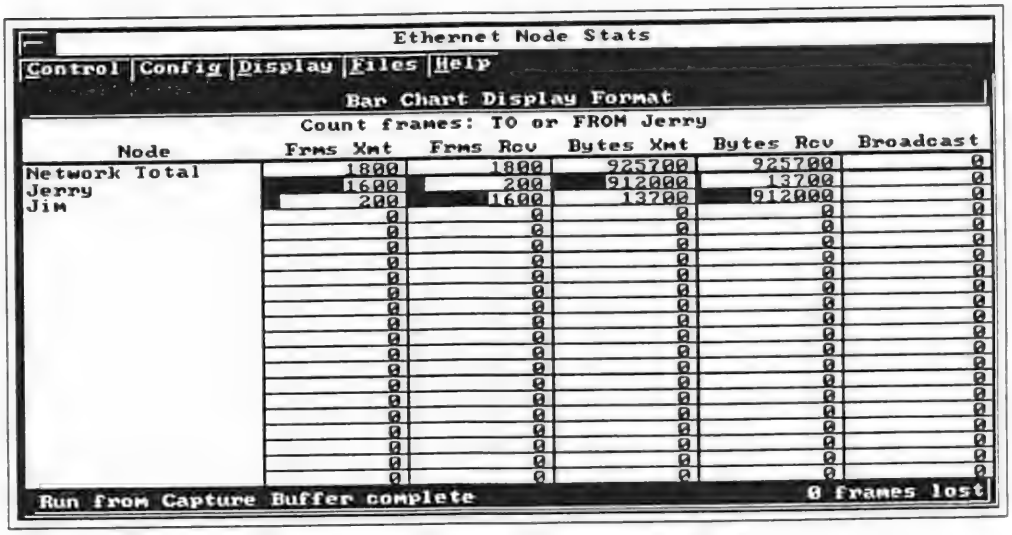
The Ethernet Summary Stats drill down capability provides fast, easy access to all statistical measurements in the Internet Advisor. Starting from the Summary Stats window, other statistical measurements can be started simply by clicking on the area of interest in Summary Stats. For example, clicking on the Protocols pie chart in Summary Stats starts the Protocol Stats measurement, or clicking on the Collisions Gauge starts Ethernet Vital Signs.

The following table lists the statistical measurements you start by clicking on selected fields in the Summary Stats window:

Summary Stats Screen Field	Measurement Started
Network Utilization	Starts Top Talkers --identifies the top talkers, so you can see who is contributing the most to the network utilization.
Collisions	Starts Vital Signs -- provides additional information as to the type of collisions occurring on the network.
Errors	Starts Top Error Sources -- displays which nodes are causing errors and what types of errors they are causing.
Node Count	Starts Node Stats -- displays statistical information for 20 nodes.
Bytes/frame	Starts Protocol Stats configured to display frame length distribution in pie-chart format.
Destination Addresses	Starts Node Stats.
Protocols	Starts Protocol Stats configured to show SAPs and Types for all protocols seen on the network.
Selected Nodes	Clicking on any one of seven nodes will start Node Stats, configured to display only frames seen to or from the selected node. Configure selected nodes with your top seven servers or nodes. This allows you to quickly see who is accessing those servers or nodes.

Note: If you are running Summary Stats from buffer, as in this example, measurements started from Summary Stats will also run from buffer. If you were to run Summary Stats from the network, then the other measurements started from Summary Stats would also run from the network. Additional information about each of the statistical measurements started from Summary Stats can be found later in this chapter. You can use the drill down function to start these measurements, or you can run the measurements individually.

4. Position your mouse on Jerry (the mouse pointer will change from a pointer to a magnifying glass) from the Selected Nodes field of the Summary Stats window and double click. Ethernet Node Stats automatically starts, configured to display only nodes to which Jerry is sending frames or from which he is receiving frames.



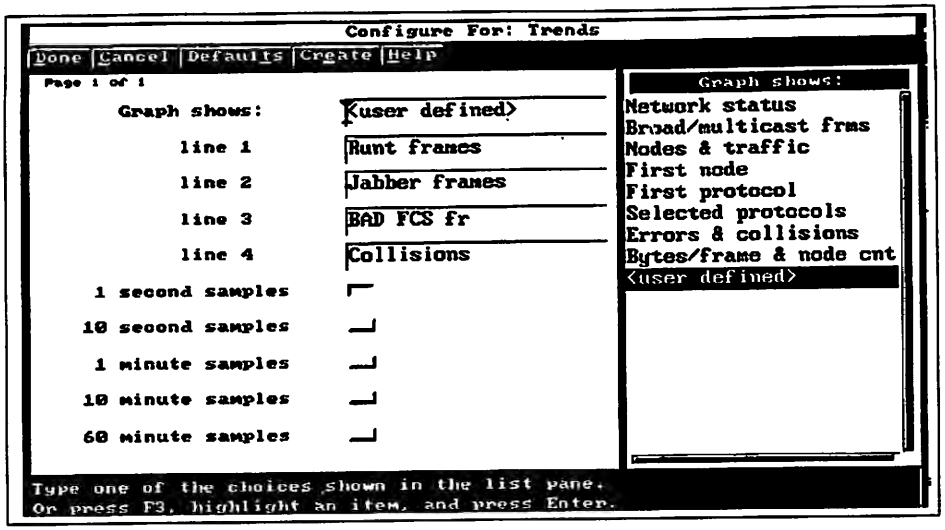
Node Stats configured to display frames to/from selected node

5. Press **[F5]** to close the Node Stats measurement.

Display Summary Stats in Graphical Format

6. From the menu bar, select **[Display | Display trends in graphical format]**.

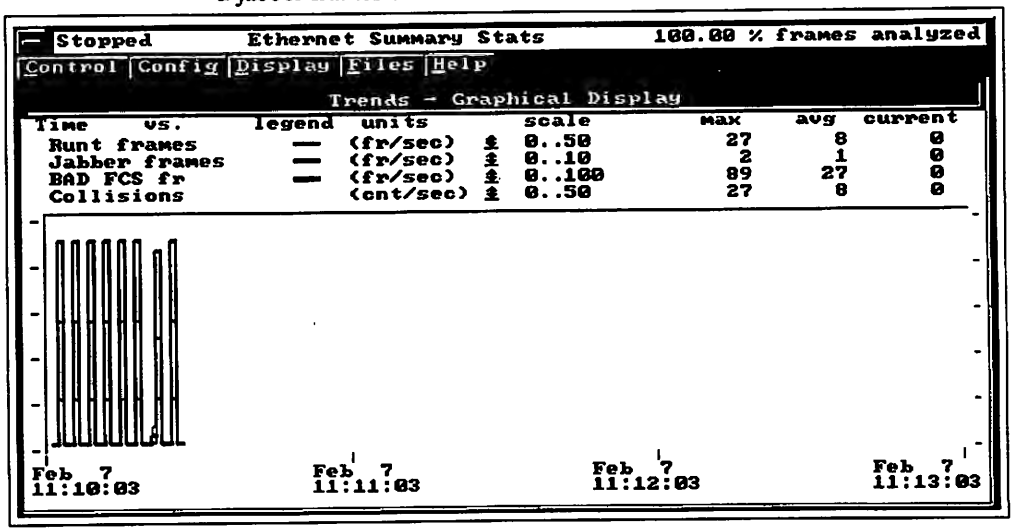
7. From the menu bar, select **[Config | Configure Trends]**. In the "Graph shows:" configuration field, select **[user defined]**. Then in the line 1, line 2, line 3, and line 4 fields, select **[Runt frames]**, **[Jabber frames]**, **[BAD FCS fr]**, and **[Collisions]**, respectively from the list pane that appears when you select each field.



Summary Stats Trends display -- configuration window

8. From the menu bar, select **[Done | Accept changes and exit]**. From the menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**. The display now shows a graph over time of the occurrence of runts, jabbers, bad FCS frames, and collisions. The network observations are peaking at:

89 bad FCS frames/second
27 runt frames/second
27 collisions
2 jabber frames/second



Summary Statistics - graphical display

Store Files Containing Statistics Data

You can save information to a comma separated variable (csv) file, and then load data from that file into the HP Internet Reporter or into a spreadsheet application such as Microsoft Excel, for further analysis.

9. From the menu bar, select **[Files | Write samples from previous run to ASCII file]** or **[Files | Log samples to ASCII file during next run]**. The File Manager window will appear.

Note: Writing samples from previous run to ASCII file will write the last 180 sample periods to disk. If you have a 1 second sample period selected, then the previous 3 minutes of statistical data will be written to disk. Logging to disk will track statistical data over time. If you log 1 second samples to disk, don't store more than 2 hours of data. Two hours of 1 second samples yields a csv file of 7,200 rows.

10. Enter a new file name in the "File name:" field, and use a "**.csv**" extension. When saving a file:
    a. You can save this file in the currently selected directory (\user\stats).
    b. Using the File commands menu bar item, you can create a new subdirectory.
    c. Using the Drive menu bar item, you can save the file to the floppy disk drive (a:).

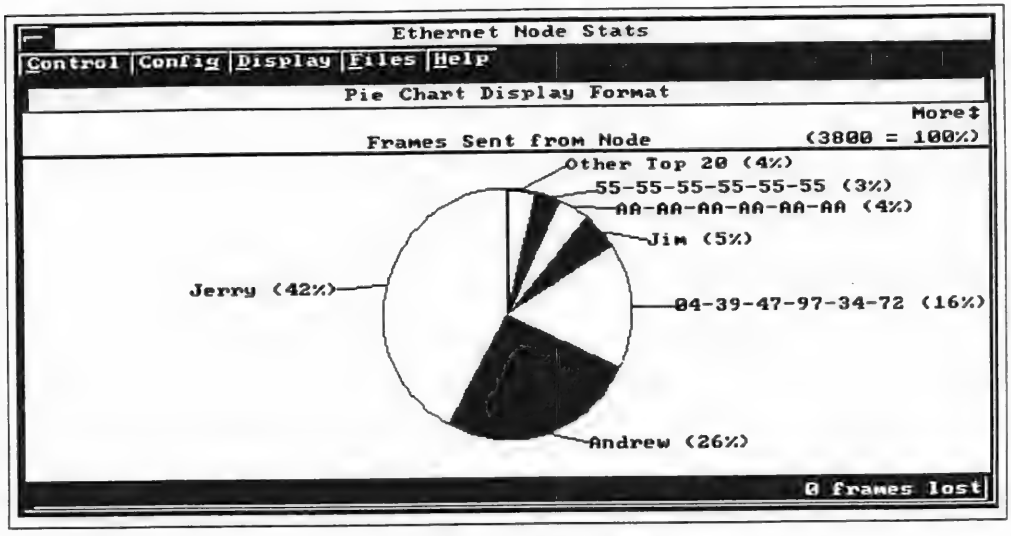
11. When you are finished naming the file, select **[Done | Accept selection and exit]**.

12. Press **[F5]** to close the Ethernet Summary Stats window.

Run Node Stats

1. From the Measurements window, Statistics category, select **[Ethernet Node Stats]** and press **[Enter]**. From the menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**.

2. From the menu bar, select **[Display | Display in pie chart format]**.



Ethernet Node Stats – pie-chart display

The Node Stats measurement, in pie-chart display format, shows statistical information for up to 20 nodes. You can display five different pie charts, depending on the selections you make in the Node Stats Configuration window.

In each pie chart, nodes are identified by their hex MAC addresses, node names, or their vendor names, depending on the format selected in the Ethernet Node Stats configuration window. For each pie chart, if a node contributes less than 2 percent of the traffic, its percentage is not shown individually. Rather, that node's percentage is shown in the "Other Top 20" section of the pie chart. The "All Other" section indicates the percentage contributed by nodes that are not in the top 20.

3. Press the **[Next Page/Prev Page]**, or **[PgUp/PgDn]** keys to toggle through the graphs. In the pie-chart, or bar-chart format, you can configure statistics to display any five of these fields:

- Frames Sent—shows the percent of frames sent from each of the top 20 nodes.
- Frames Received—shows the percent of frames received at each node.
- Bytes Sent—shows the percent of bytes sent from each node.
- Bytes Received—shows the percent of bytes received at each node.
- Broadcast Sent—shows the percent of broadcasts sent from each node.
- Multicast Sent—shows the percent of multicasts sent from each node.
- Errors Sent—shows the percent of error frames sent from each node.

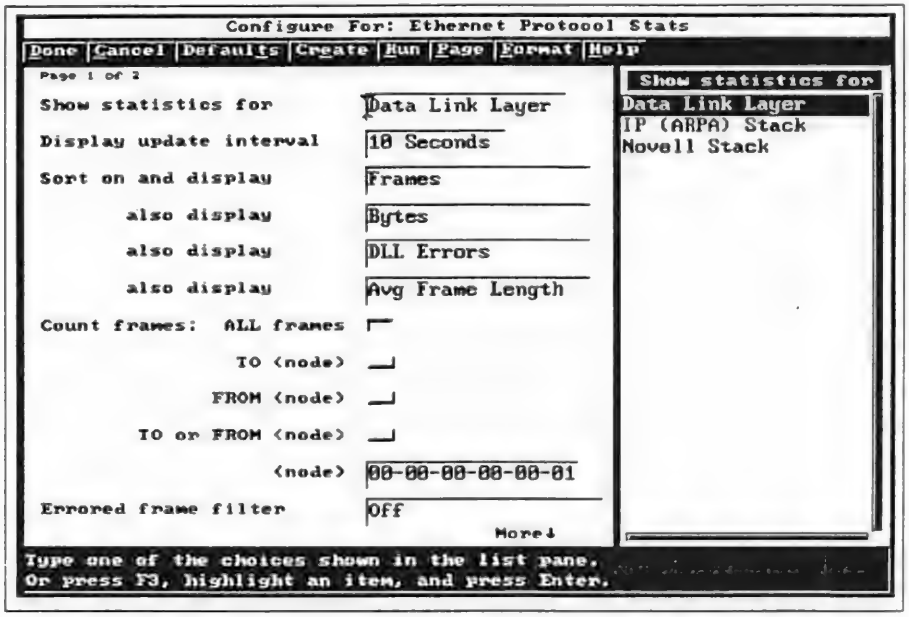
4. From the menu bar, select **[Config | Configure Ethernet Node Stats]** and explore the capability to sort on a display according to user-specified needs. When you are finished, select **[Done | Accept changes and exit]** from the menu bar.

5. Press **[F5]** to close the Node Stats measurement.

Run Protocol Stats

1. From the Measurements window, Statistics category, select **[Ethernet Protocol Stats]** and press **[Enter]**.

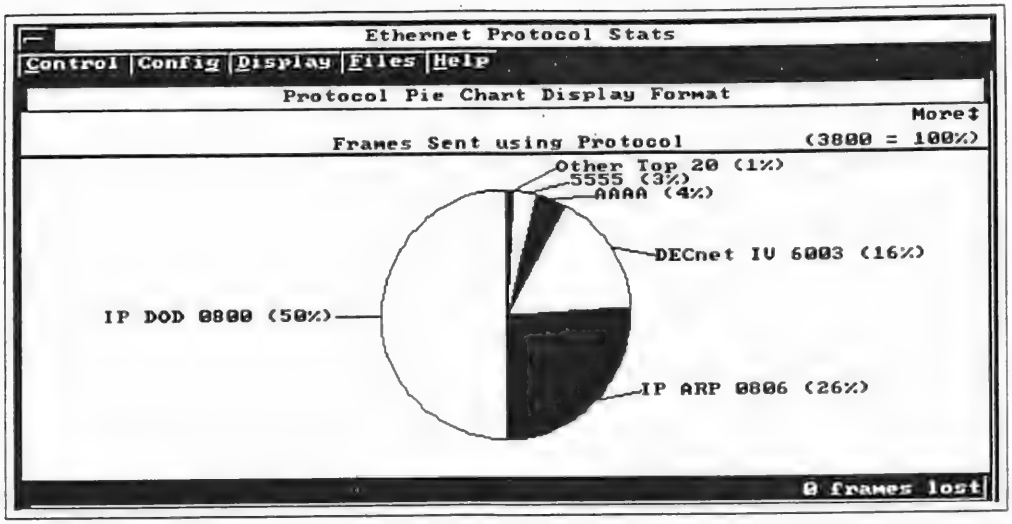
2. From the menu bar, select **[Config | Configure Ethernet Protocol Stats]**. From the menu bar, select **[Defaults | Restore default values]**. From the menu bar, select **[Done | Accept changes and exit]**.



Protocol Stats – Configuration window

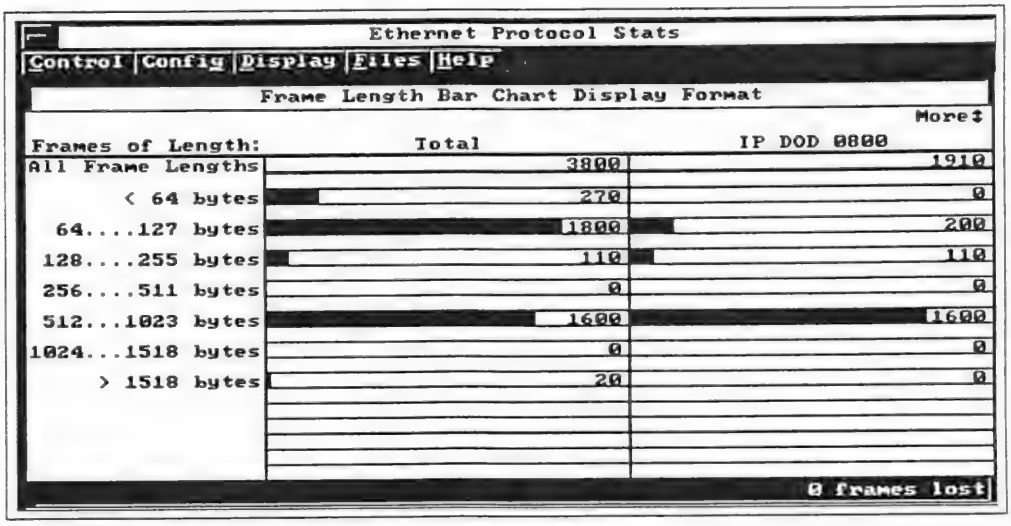
3. From the menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]** to review information on the protocols running on your network.

4. From the menu bar, select **[Display | Display protocols in pie chart format]**. Use the **[Next Page/Prev Page]** or **[PgDn/PgUp]** keys to toggle through additional data.



Protocol Stats displayed in pie-chart format

5. From the menu bar, select **[Display | Display frame lengths in bar chart format]** to review frame length distribution by protocol. You can also toggle between screens in this display.



Frame Length Distribution in bar-chart format

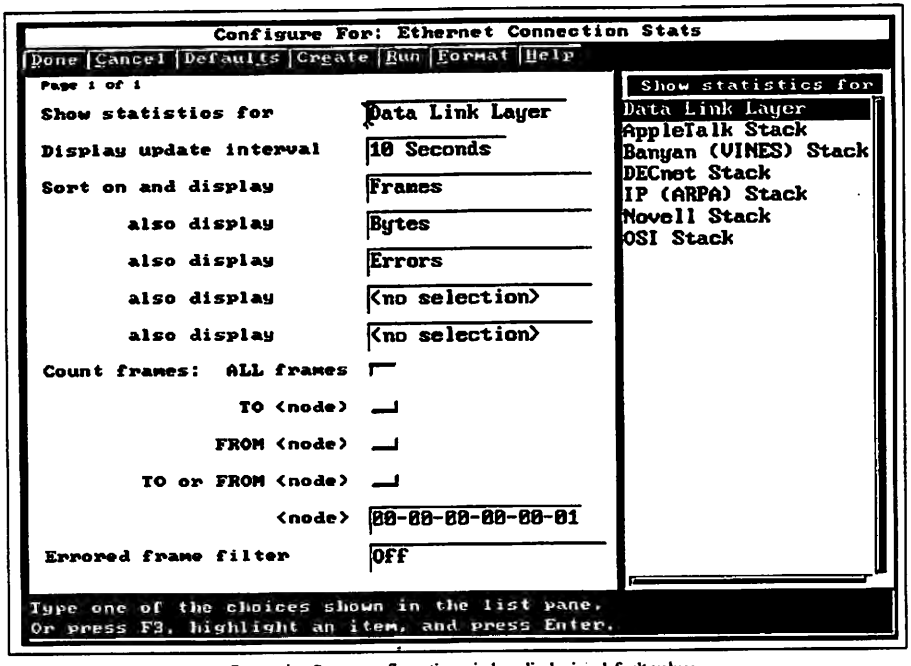
6. The Files selection can be used to save protocol and frame length data to a csv file. That file then can be imported into the HP Internet Reporter or into a spreadsheet application such as Microsoft Excel.

7. Press **[F5]** to close the Protocol Stats measurement.

Run Connection Stats

1. From the Measurements window, Statistics category, select **[Ethernet Connection Stats]** and press **[Enter]**.

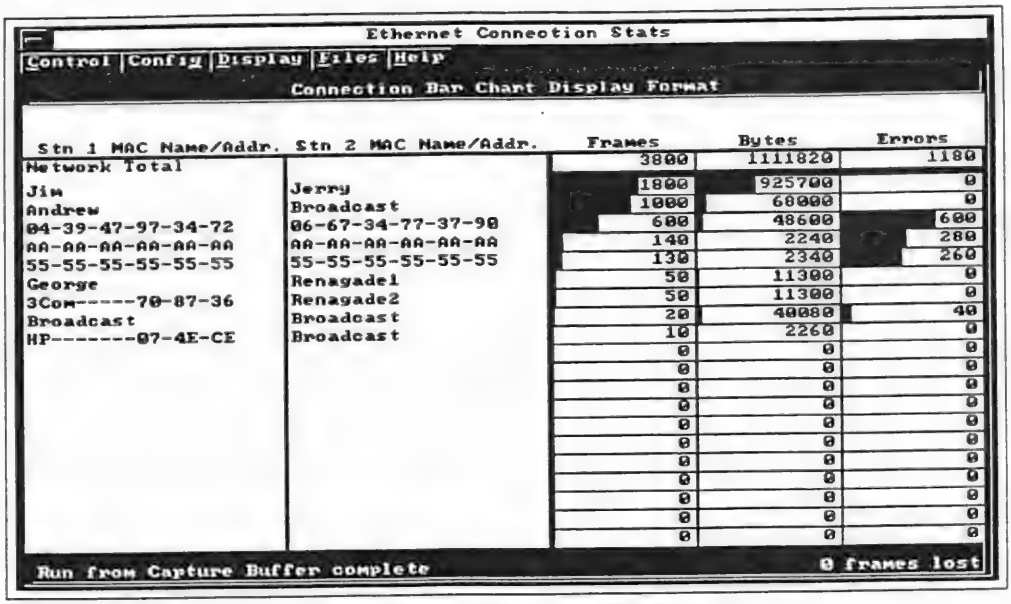
2. From the menu bar, select **[Config | Configure Ethernet Connection Stats]**. From the menu bar, select **[Defaults | Restore default values]**.



Connection Stats –configuration window displaying default values

3. Select **[Done | Accept changes and exit]** from the menu bar.

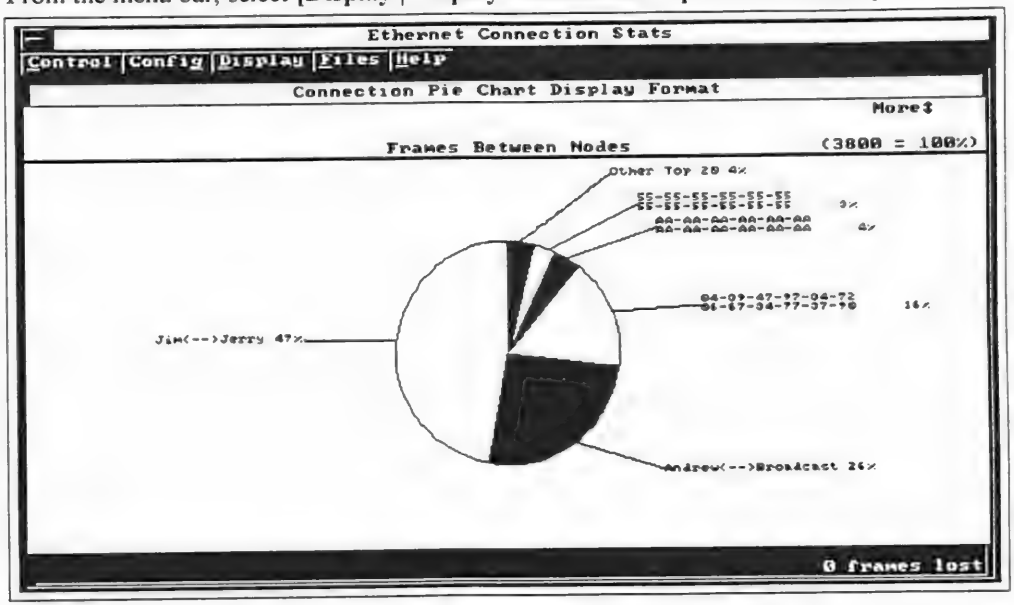
4. From the menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**.



Connection Stats – MAC level conversations displayed

In the example above, MAC layer conversations are displayed. Total frames, bytes and errors are displayed. This information can be viewed in percentages too.

5. From the menu bar, select **[Display | Display connections in pie chart format]**.



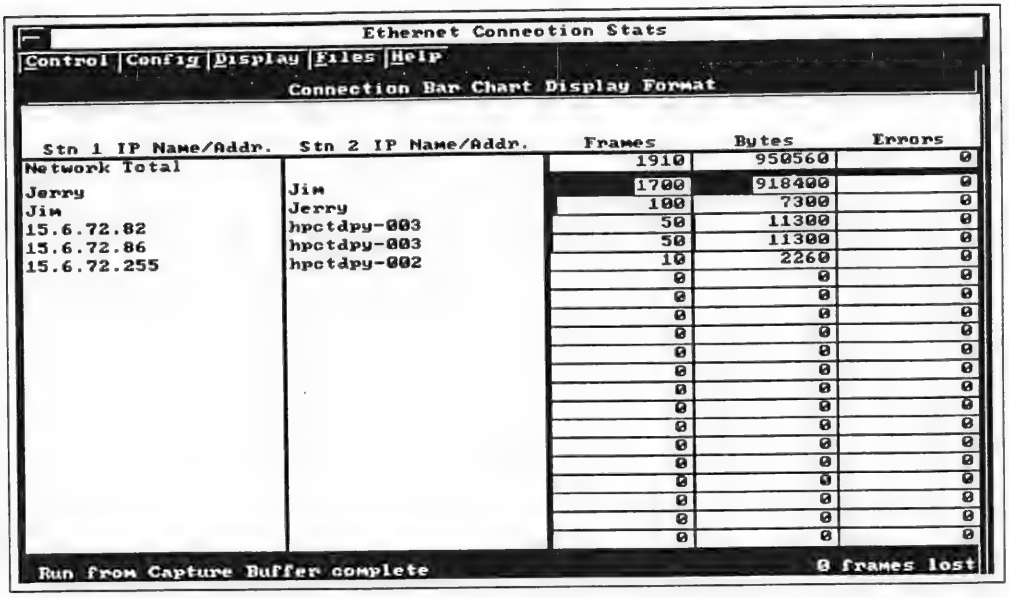
Connection Stats – pie-chart format

Use the down arrow key to toggle between all the pie charts available.

6. From the menu bar, select **[Display | Display connections in bar chart format]**.

7. Select **[Config | Configure Ethernet Connection Stats]**. In the "Show statistics for:" configuration field select **[IP (ARPA) Stack]**. From the menu bar, select **[Done | Accept changes and exit]**.

8. From the menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**.



Connection Stats – IP layer connections displayed

9. Press **[F5]** to close the Connection Stats measurement.

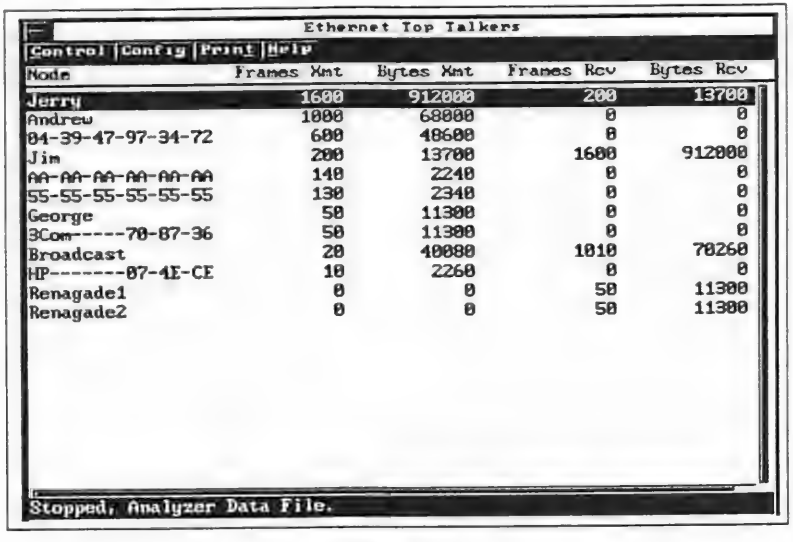
Note: IP Subnet Connection Stats is available from the Statistics category too. This measurement is identical to Connection Stats, however, connections between IP subnets are displayed. Subnet addresses and subnet masks can be configured in the configuration window for IP Connection Stats.

Run Top Talkers

The Ethernet Top Talkers measurement displays a list of up to 50 nodes that have generated the most frames since the measurement was started.

1. From the Measurements window, Statistics category, select **[Ethernet Top Talkers]** and press **[Enter]**. From the menu bar, select **[Config | Configure measurement]**. Set the Update Interval to **[10]** and the Errored frame filter to **[Off]**. From the menu bar, select **[Format | Display addresses by node/station name]** and press **[Enter]**. From the menu bar, select **[Done | Accept changes and exit]**.

2. From the Ethernet Top Talkers menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**.



Top Talkers window

Top Talkers displays the following information about each node:

- **Node**—shows either the hex MAC address, node name, or vendor name of each node, depending on the format selected in the Top Talkers configuration window.
- **Frames Xmt**—shows the number of frames each node sent since the measurement started.
- **Bytes Xmt**—shows the number of bytes each node sent since the measurement started.
- **Frames Rcv**—shows the number of frames sent to each node since the measurement started.
- **Bytes Rcv**—shows the number of bytes sent to each node since the measurement started.

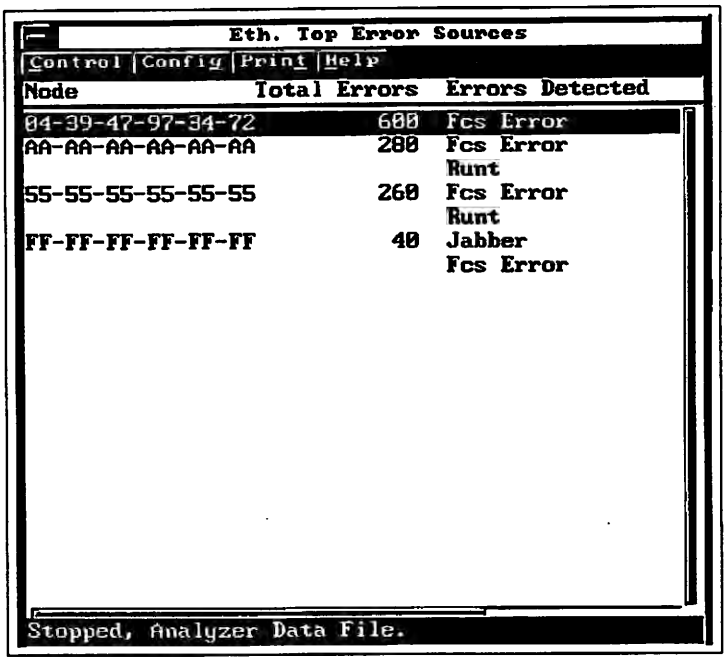
3. Press **[F5]** to close the Top Talkers measurement.

Note: Top Talkers can be printed to a file and imported into the HP Internet Reporter.

Run Top Error Sources

1. From the Measurements window, Statistics category, select **[Eth. Top Error Sources]** and press **[Enter]**.

2. From the menu bar, select **[Config | Configure measurement]**. Set the Update Interval to **[10]** and set the Ignore Runt Errors field to **[No]**. From the menu bar, select **[Done | Accept changes and exit]**. From the menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**.



Top Error Sources window

Note: The nodes with addresses AA-AA-AA-AA-AA-AA or 55-55-55-55-55-55, in the example above, are actually collision fragments. That is why they are displayed as a runt with a bad FCS.

3. Press **[F5]** to close the Top Error Sources measurement.

Chapter Notes

Chapter Notes

Chapter 6 - Vital Signs

Objective

Isolating a LAN problem or tuning a network can often mean searching through thousands of captured frames, most of which are insignificant or irrelevant. Using the Vital Signs measurements in the HP Internet Advisor for Ethernet will increase your productivity and save you time by automating the processing of this information and helping you determine what is important and what is not.

Vital Signs provide a statistical picture of the Ethernet MAC layer, Novell, TCP/IP, AppleTalk, Banyan, DECnet, and OSI protocol stacks. Vital Signs can be used to identify problems or assist in optimizing the configuration of network components and software to get the most out of your network. Current, average, peak, and total sample values are shown for each statistical parameter, along with user-configurable thresholds that can be set dynamically to automatically detect intermittently occurring events.

When a threshold is exceeded, it can be recorded in the event log and can be used to stop the capture process so that events leading up to the problem can be analyzed when convenient for you. Vital Signs are the first step in an expert process which also uses Commentators and specific frames stored in the capture buffer to detect and resolve your networking problems.

Vital Signs operate in real time, interpreting data traffic as it occurs. The thresholds in Vital Signs automatically stops all measurements from running when configured for specific significant events that occur, allowing you time to analyze the problem.

In this chapter, you will learn to configure and use the Vital Sign measurements and decodes to become more productive at troubleshooting and managing your network.

Topics Covered

- Configuration of the thresholds and trigger actions
- Examining the capture buffer after a Vital Sign measurement stops
- Using Detailed and Summary Decodes to analyze errored frames
- Using Novell Vital Signs
- Using decodes to analyze specific Novell frames
- Using TCP/IP Vital Sign measurement to analyze Ethernet and ARPA frame types
- Using ARPA stack decodes to analyze both Telnet and FTP operations
- Using DECnet Vital Signs
- Help text for Vital Signs

Preparation

- Internet Advisor for Ethernet should not have any measurements running.
- The Measurements window is properly sized and the categories are fully expanded.
- The Node List **c:\user\class\class.lst** should be loaded.
- The Advisor Data File **c:\user\class\evit.eth** should be loaded into the capture buffer.

Vital Sign Measurements

Vital Sign measurements display performance statistics and are available for Ethernet, TCP/IP, Novell, DECnet, AppleTalk, OSI, and Banyan. You see exactly what kinds of traffic are present, and their performance percentages. Data is simultaneously captured in the capture buffer as the various Vital Sign measurements are executed.

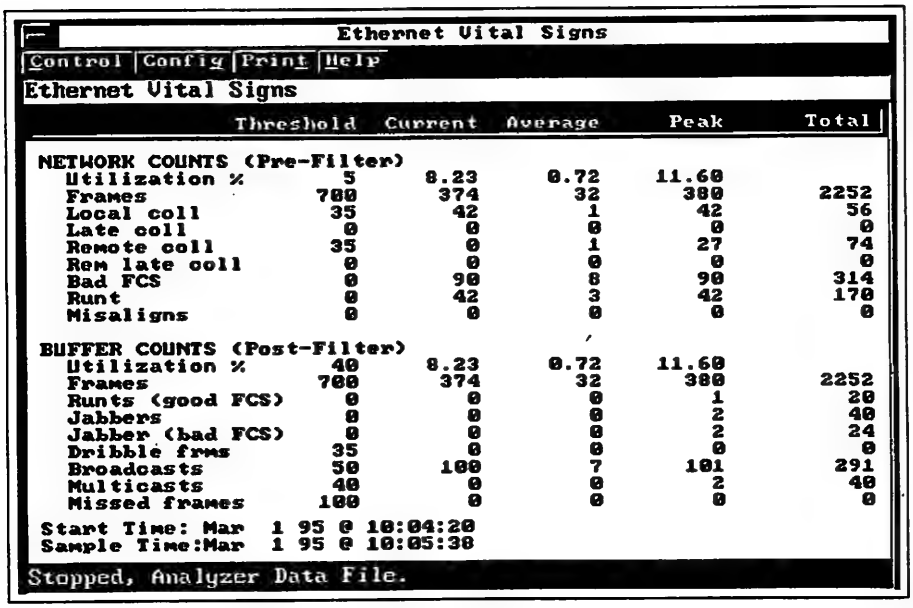
The unique interaction between Vital Signs and Packet Capture is that the Vital Signs window is driven by the frames arriving into the capture buffer.

- Using the Vital Signs configuration menus, you can set thresholds to insert performance events into the Event Log.
- You can also set a threshold which, when exceeded, stops all measurements. Typically, you may choose to use a decode to examine frames that caused this event, or replay data through statistical measurements to document the network's behavior just before the threshold was exceeded.

Run Ethernet Vital Signs

1. From the Measurements window, Statistics category, select the **[Ethernet Vital Signs]** and press **[Enter]**.

2. Run Ethernet Vital Signs from the capture buffer by selecting **[Control | Run Measurement From Capture Buffer | All Frames]**.

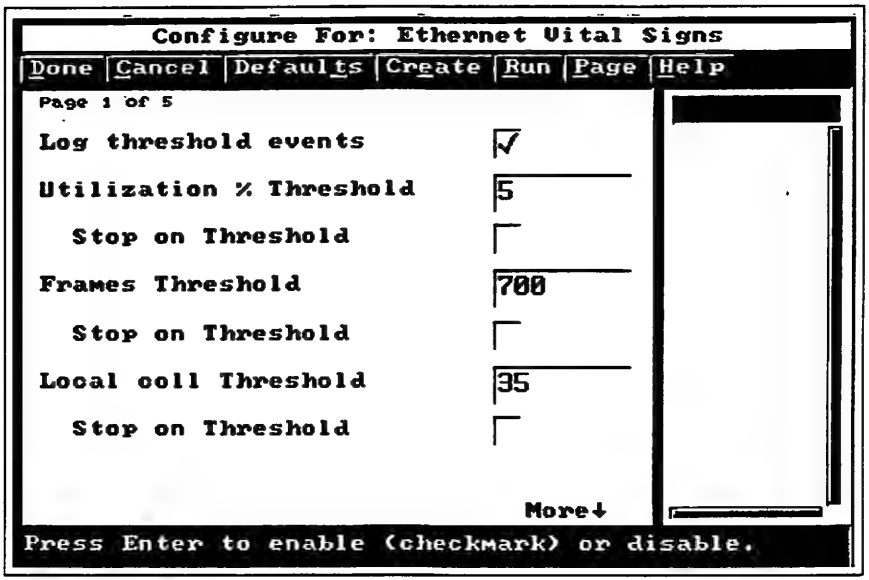


Ethernet Vital Signs window

Notice in the Ethernet Vital Signs results that there are several types of Ethernet media access control events. When thresholds are exceeded, results may be displayed in orange or red, depending on whether a threshold and/or a trigger has been set, within the current column.

Exceeded thresholds are also recorded by the event log. The Ethernet Vital Signs configuration screen allows you to specify threshold values, and when the threshold value is exceeded the event log will record the excessive "peak" value and the time that the threshold was exceeded.

3. In the Ethernet Vital Signs window, select **[Config | Configure measurement]** from the menu bar. Configure Ethernet Vital Signs to have the same threshold values as in the example below. When finished from the menu bar, select **[Done | Accept changes and exit].**



Ethernet Vital Signs – Configuration Screen

The ***Log threshold events*** selection on the configuration page of the Vital Signs measurement inserts entries into the Event Log. Threshold values can be specified for the particular network environment. The ***Stop on Threshold*** selection does one of the following:

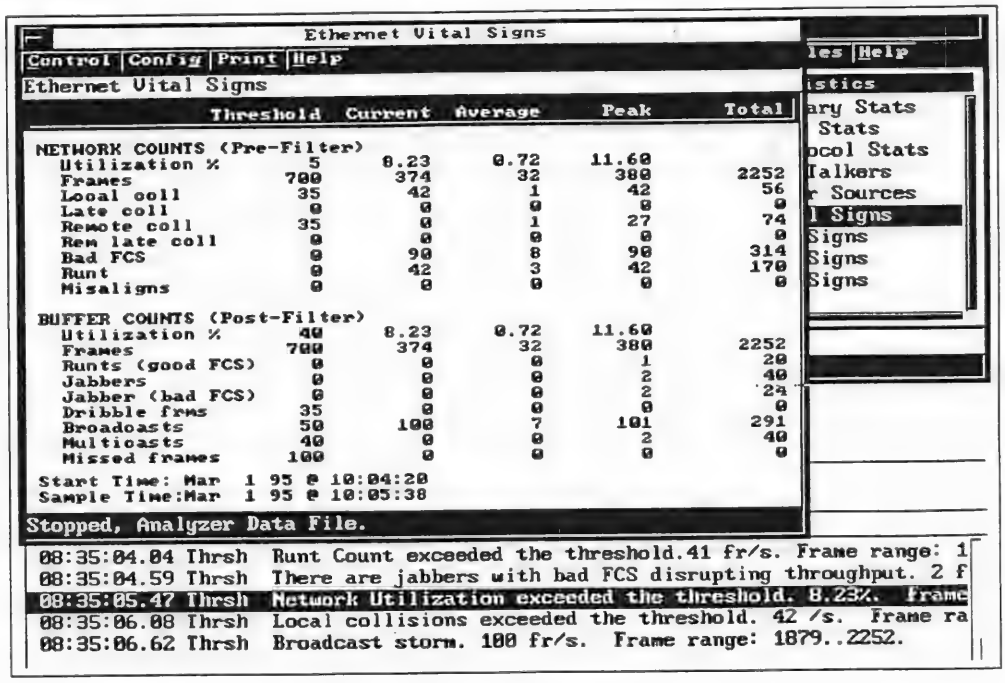
If unselected, the Internet Advisor continues to monitor the network and posts Vital Signs statistics until you manually stop the measurement.

If selected, the Internet Advisor stops the measurement when the threshold is exceeded, preserving the data capture buffer to allow you to analyze frames with a decode or replay the buffer through other statistical measurements.

4. Press **[F7]** to open the Events Browser, then select **[Browse | Browse All Events]** from the menu bar. Iconize the Event Log by clicking on it, then press **[F4 | I]**. Position the Event Browser and the Ethernet Vital Signs as in the example below. With the Window Control **[F4]** you can select to move and size the active window.

Refer to the *HP LAN Advisor Family Quick start/User's Guide (part. no. 5963-2720)* for more information on managing Advisor windows.

5. Re-run the Vital Signs by selecting **[Control | Run Measurement From Capture Buffer | All Frames]**.



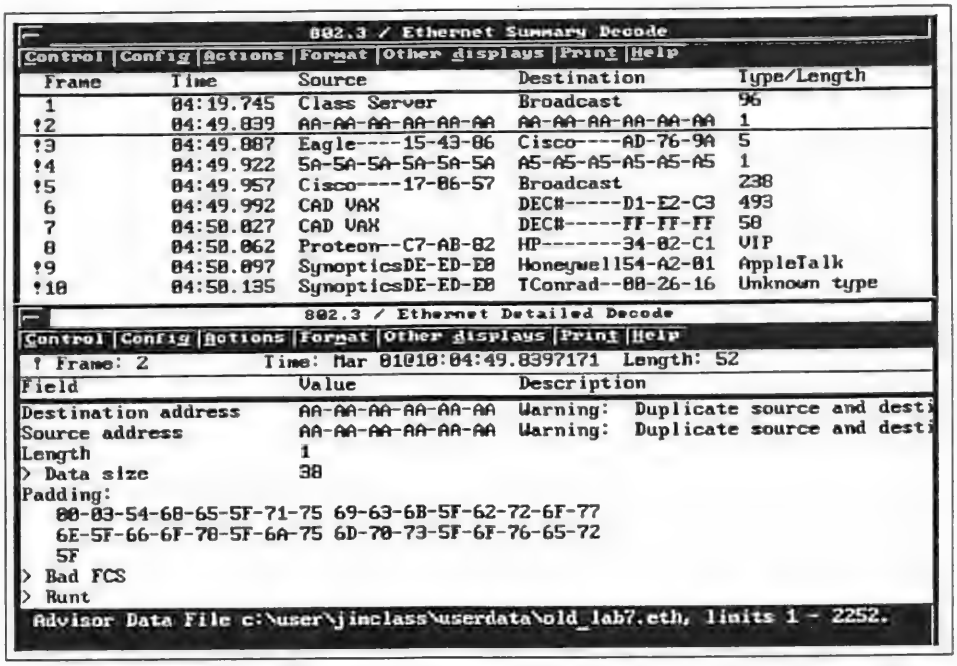
Ethernet Vital Signs with All Events Browser

The events that exceeded the threshold in the previous screen were entered into the All Events Browser. Notice the entries for thresholds that were configured under the Ethernet Vital Signs configuration screen.

6. From the Ethernet Vital Signs window, press **[F5]** to close. From the All Events Browser window, press **[F5]** to close.

7. In the Measurements window, double click on the Decodes category to expand it, until you see Ethernet/LLC. Click once on the **[Ethernet/LLC]** category then click once to select the **[802.3/Ethernet Decode]**.

8. From the 802.3/Ethernet Detailed Decode window, select **[Other displays | Open Summary Decode window]** from the menu bar. Move and size the two windows to appear as in the following example:



802.3/Ethernet Detail and Summary Decodes

In the previous example, you started running Vital Signs, and because the Internet Advisor for Ethernet can simultaneously capture data and post vital sign statistics, you stopped the Vital Signs measurement and reviewed the frames that caused the Local Collision threshold to be exceeded.

Using two decode windows, the Ethernet Summary Decode window displays errored frames in the left-hand column by marking these frames with "!" (for example, frame 2).

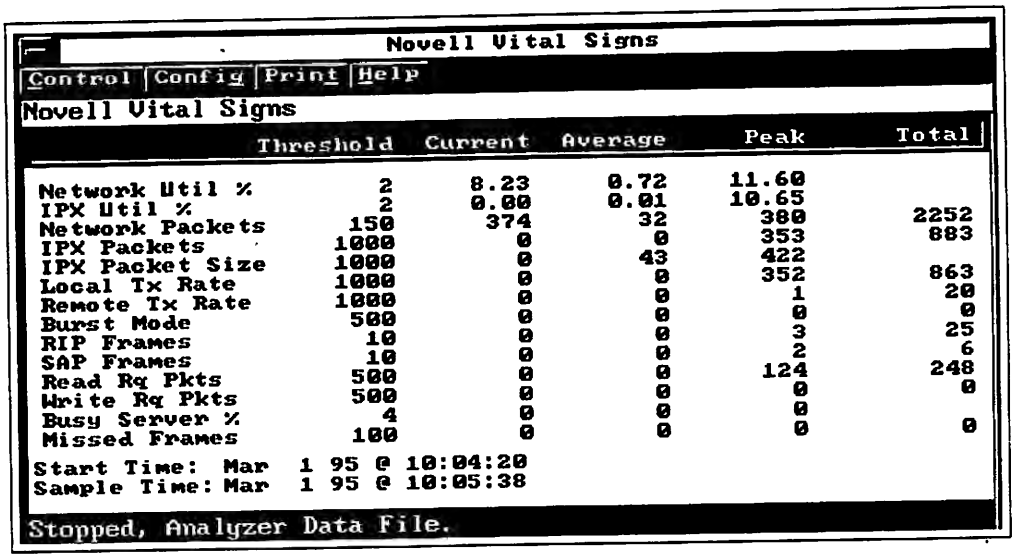
The Ethernet Detailed Decode window displays frame 2 in two ways: first by marking it with an "!"; second, at the bottom of the display, important information about the frame is clearly shown: it is a runt and has a bad FCS value.

> **NOTE**: Frames with a source and destination address of all "A"s or "5"s indicate a collision frame. The jam signal associated with collisions is alternating "1"s and "0"s which, when framed as 8 bits, are either "10101010" which is equal to 10 or Hex A, or "01010101" which is equal to 5 or Hex 5.

9. Close the Detail and Summary Decodes by pressing **[F5]** twice.

Run Novell Vital Signs

1. From the Measurements window, Statistics category, select **[Novell Vital Signs]** and press **[Enter]**. Run Novell Vital Signs from the capture buffer by selecting **[Control | Run Measurement From Capture Buffer | All Frames]**.



Novell Vital Signs window

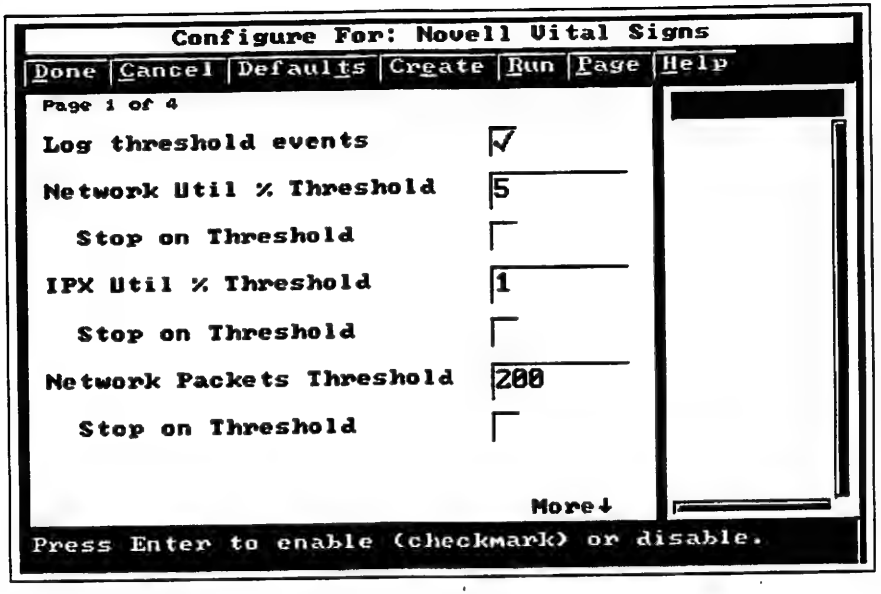
The Novell Vital Signs measurement provides you with an accurate view of Novell frame characteristics, along with network and Novell IPX utilization. Vital Signs display the kinds of events occurring as the frames enter the capture buffer. Results of utilization, packet type, and packet size measurements track how your network is utilized. The local and remote transmit rates inform you where the frames are originating. In this example, the Internet Advisor is observing from the local segment. You could relocate the Internet Advisor to gain additional insight into frame propagation across strategic network components.

The burst mode results indicate whether any of the Novell nodes are using burst operations to send multitudes of frames in a sequence, as opposed to the usual way of acknowledging frames individually.

Using a filter to focus on a Novell server, you could analyze, the amount of read and write requests being handled over a time period. Additionally, information about busy server frames and percentages could assist the network manager in optimizing or tuning server utilization.

2. In the Novell Vital Signs window, select **[Configure | Configure measurement]** from the menu bar.

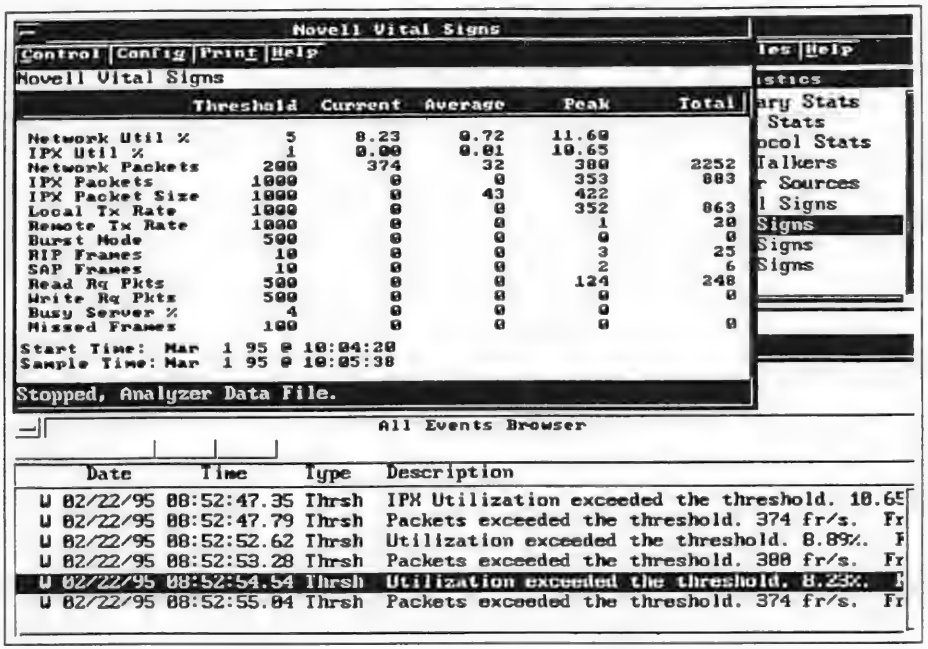
3. Configure the Network Utilization % Threshold for **[5%]**, the IPX Utilization % Threshold for **[19%]**, and the Network Packets Threshold to **[200]**. Select **[Log threshold events]**. Select **[Done | Accept changes and exit]**.



Novell Vital Signs Configuration window

4. Double click on the **EVENTS Icon**, or press **[F7]** to open the Event Log. From the menu bar, select **[Browse | Browse All Events]**. Position the All Events Browser window into the lower left-hand side of the display and then size the window as shown in the example on the following page. Iconize the Event Log by pressing **[F4 | I]**.

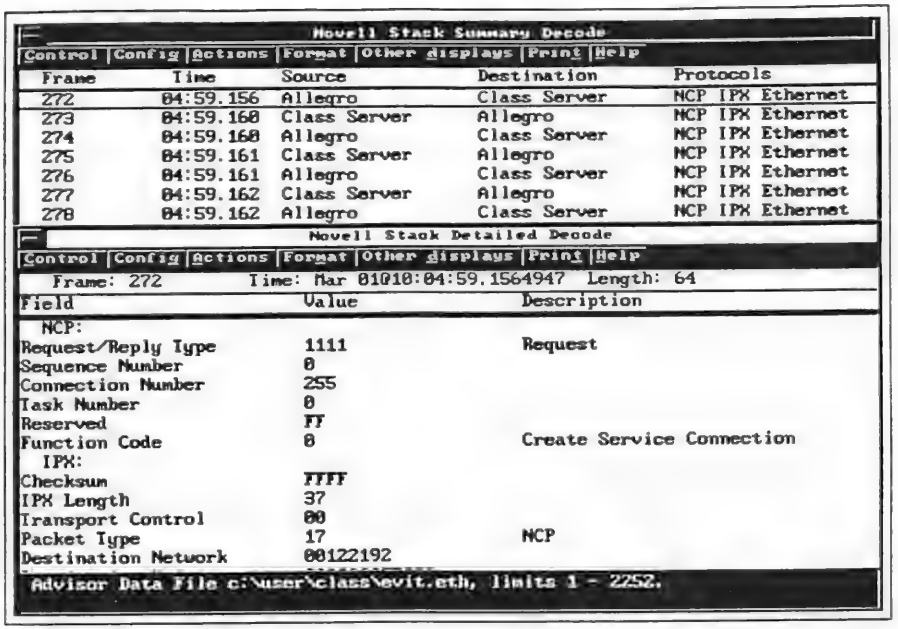
5. From the Novell Vital Signs window, select **[Control | Run Measurement From Capture Buffer | All Frames]**.



Novell Vital Signs and All Events Browser

6. Notice that the thresholds were exceeded and posted to the All Events Browser. Close the Novell Vital Signs and the All Events Browser by pressing **[F5]**.

7. In the Measurements window Decodes category, click twice on **[Novell Stack Decode]**. From the menu bar, select **[Other display | Open Summary Decode window]**. Move and size the Novell Stack Summary Decode to the top of the screen and move and size the detailed decode to the bottom of the screen.



Novell Stack Summary and Detailed Decode windows

8. From the Novell Stack Detail Decode window, select **[Actions | Go to frame | Frame # 272]**.

The Novell Stack Summary Decode window displays error-free Novell traffic. If errored frames were present, they would be marked in the left-hand column with "!". You can use the Up/Down arrow keys to move from frame to frame and to review the file transfer between Allegro and Class Server.

9. Press **[F5]** to close the decode windows.

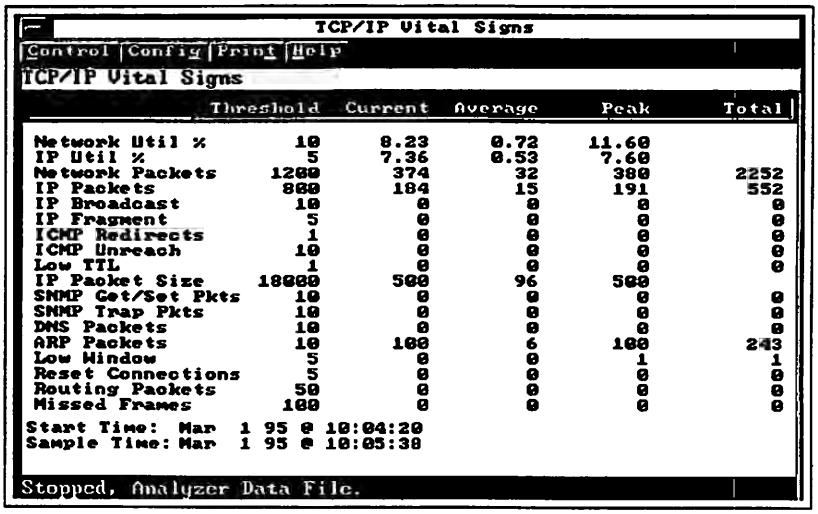
Run TCP/IP Vital Signs

Use the TCP/IP Vital Signs measurement to observe the network when a Telnet connection has been made.

1. From the Measurements window, Statistics category, select **[TCP/IP Vital Signs]** and press **[Enter]**.

2. From the menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**.

Note the count of ARP frames, and DNS frames if a name lookup was done from a UNIX(R) station to the Domain Name Server that occurred after the login. The ARP frames are part of the process of resolving IP network addresses to MAC level physical addresses.

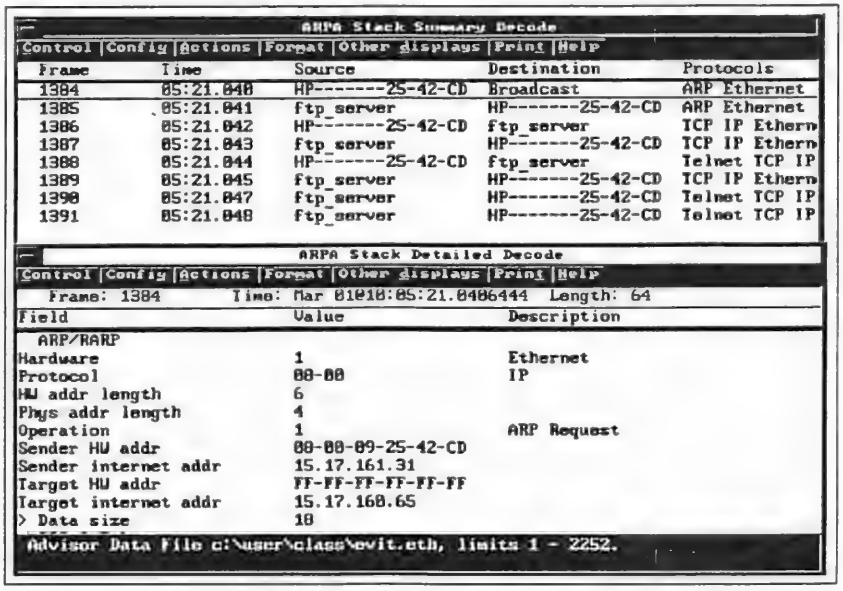


TCP/IP Vital Signs window

Note the IP packet size field. This is the average packet size seen on the connection. If this were only Telnet data, it would be small because Telnet sends single characters across its TCP connection as the user types.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Limited.

3. Press **[F5]** to close the Vital Sign measurement. In the Measurements window, Decodes category, click twice on the **[ARPA Stack Decode]**. From the menu bar, select **[Other displays | Open Summary Decode window]**. Move and size windows to look like the following example. Go to frame 1384 by selecting **[Actions | Go to Frame | Frame # 1384]**.



TCP/IP Detail and Summary Decode windows

4. From the ARPA Stack Detail Decode window press **[F4 | Z]** to zoom the window. Use the Up/Down arrow keys to review the Telnet connection from the ARP Request/Reply through the TCP Connect process, the Telnet Data Transfer and finally, through the TCP Disconnect process (frames 1384 through 1403). When you are finished, close the decode windows by pressing **[F5]**.

Note: TCP/IP Vital Signs can be used to monitor the network for abnormal conditions such as: Broadcast storms; ICMP redirects (misconfigured nodes), Low TTL (time to live), excessive amounts of SNMP packets, Low Windows (flow control), and Reset Connections (abnormal TCP termination).

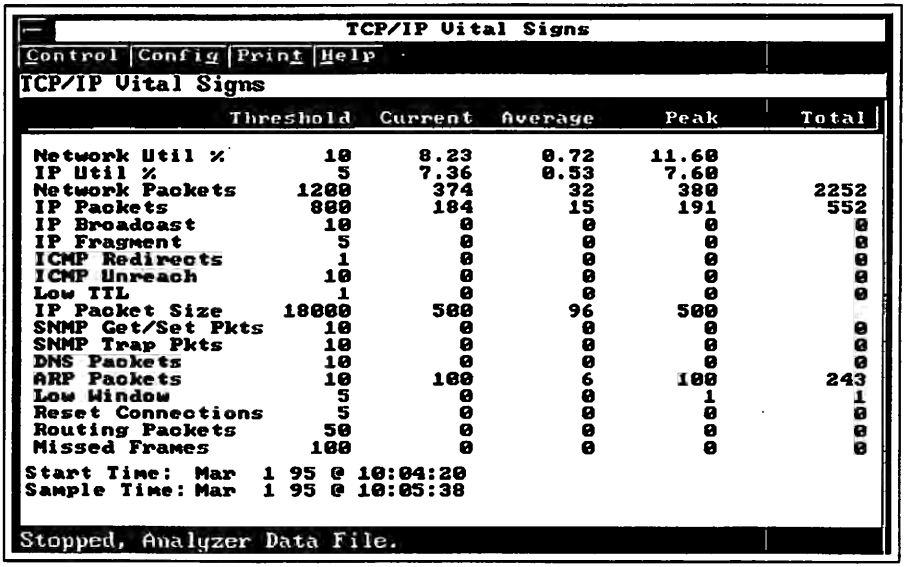
Understanding Normal FTP Operation

Use the TCP/IP Vital Signs measurement to observe the network during an FTP login, file transfer, and logout.

1. From the Measurements window, Statistics category, select **[TCP/IP Vital Signs]** and press **[Enter]**.

2. Run TCP/IP Vital Signs from buffer by selecting **[Control | Run Measurement From Capture Buffer | All Frames]**.

3. Note the count of ARP frames, and DNS frames if a name lookup was done from a UNIX station to the Domain Name Server that occurred after the login. The ARP frames are part of the process of resolving IP network addresses to MAC level physical addresses.

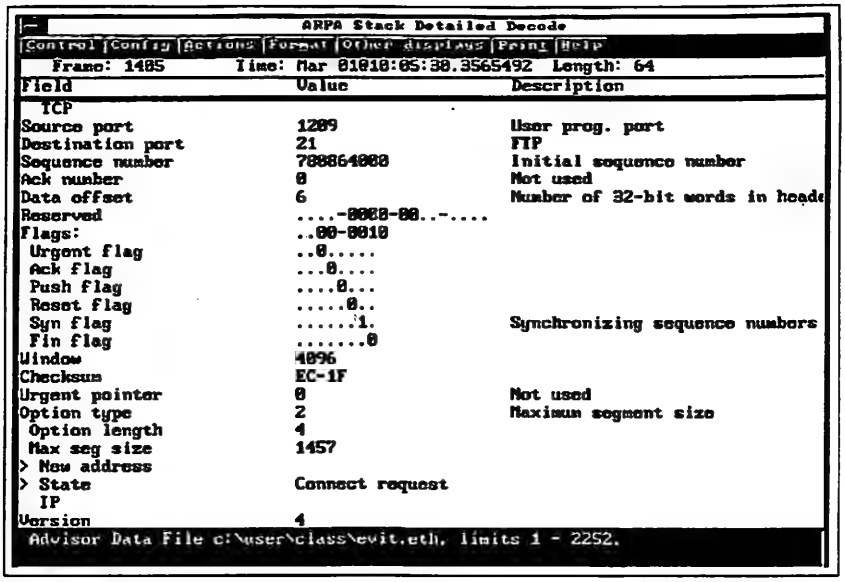


TCP/IP Vital Signs window

Both FTP and Telnet applications require the same overhead in setting up their TCP connections. FTP is complicated because it sets up two connections when an actual file is transferred: one control connection that transfers commands to/from the user (the `put` command tells the other FTP agent to prepare for a file transfer, etc.); and one data connection that carries the actual file data.

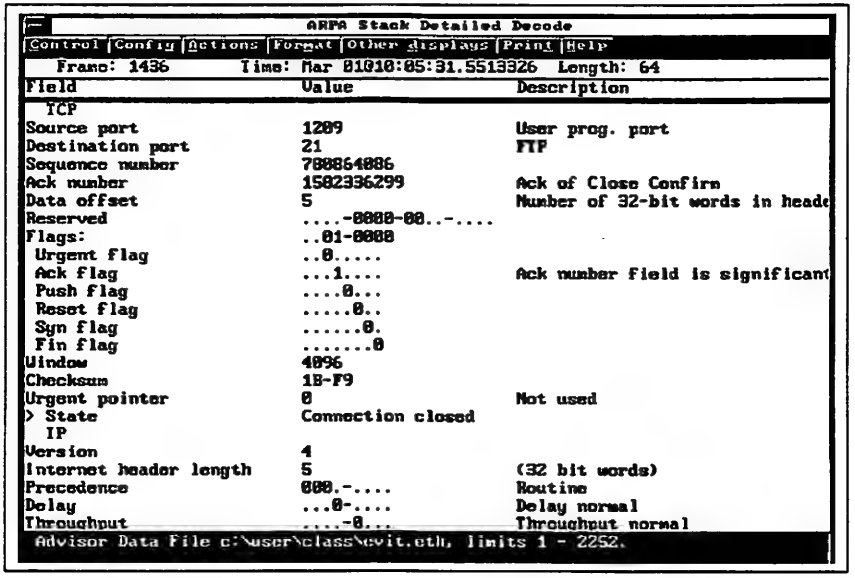
Note the IP packet size field. This is the average packet size seen on the connection. It should be larger than that seen for Telnet because FTP sends full commands and files across its TCP connection.

4. Press **[F5]** to close the Vital Sign measurement. From the Measurements window, Decodes category, double click on the **[ARPA Stack Decode]**. Zoom decode window **[F4 | Z]**. Go to frame 1405 by selecting **[Actions | Go to Frame | Frame # 1405]**.



ARPA Stack Decode – frame 1405 displayed

5. Use the Up/Down arrow keys to review the FTP connection from the TCP Connect process through the FTP Data Transfer, and finally, through the TCP Disconnect process.



ARPA Detailed Decode – FTP connection closed

NOTE: While following the TCP connection, you will see frames with errors (exclamation mark next to the frame number). Also, note that there are two sets of TCP connects and disconnects.

6. Press **[F5]** to close the decode windows.

Run DECnet Vitals

1. The Advisor Data File **c:\user\class\decnet.eth** must be loaded into the capture buffer.

NOTE: The data contained in the decnet.eth data file was created in a lab environment. Actual DECnet data may be different. This file was created to trigger all the DECnet Commentator events and many DECnet Vital Signs events.

2. From the Measurements window, Statistics category, select **[DECnet Vital Signs]** and press **[Enter]**. Run DECnet Vital Signs from the buffer by selecting **[Control | Run Measurement From Capture Buffer | All Frames]**.

DECnet Vital Signs

Control | Config | Print | Help

DECnet Vital Signs

	Threshold	Current	Average	Peak	Total
Network Util %	10	0.00	0.00	8.16	
DRP Util %	5	0.00	0.00	4.05	
LAT Util %	5	0.00	0.00	0.16	
MOP Util %	5	0	0	0	
LAVC Util %	5	0	0	0	
Network Packets	1200	1	0	253	383
DRP Packet Size	18000	0	4	1457	
DRP Data Msgs	100	0	0	149	184
DRP Control Msgs	10	0	0	10	10
DRP RTS Packets	10	0	0	1	2
DRP Hi. Visit Ct	1	0	0	1	2
NSP Fragments	100	0	0	25	31
NSP Retrans CI	5	0	0	13	13
DECU Util. %	5	0.00	0.00	4.10	
DECU Packet Sz	1500	71	9	545	
CLNP Error PDU	10	0	0	2	2
DECU Data PDU	100	1	0	92	110
DECU Low Lifetime	5	0	0	2	2
TP Error PDU	10	0	0	1	1
DECU Low Credit	5	0	0	3	9
DECU Fragments	100	0	0	22	22
Missed Frames	100	0	0	0	0

Start Time: Jun 22 94 @ 8:23:35
Sample Time: Jun 22 94 @ 8:33:53

Stopped, Analyzer Data File.

DECnet Vital Signs window

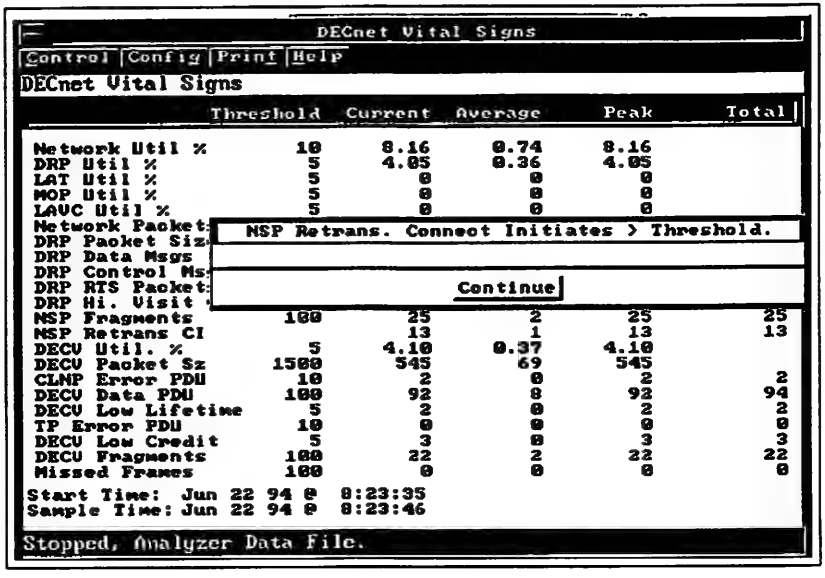
The DECnet Vital Signs measurement provides an accurate view of DECnet frame characteristics, along with network and DECnet utilization. DECnet Vital Signs displays the events that are occurring as they are captured into the capture buffer.

Some particular events to review from the example above are the number of DRP data messages versus the number of DRP control messages. There should be a much higher number of data messages (real user data frames) than control messages (routing and control messages).

Another event to review from the example above is the NSP Retrans CI. These are Retransmitted Connect Initiate frames. If the number is high, it can indicate a problem with your network, your server, or your end user. If the count is high you can troubleshoot further by using the DECnet Commentator measurement, which shows which nodes are involved. This is important in troubleshooting this problem. If you notice that many users are sending multiple Connect Initiates to one server, then that server is probably overloaded. If just one user is sending multiple Connect Initiates to one or more servers, then the problem is most likely in the end node. However, if many nodes are sending Connect Initiates to several servers, then poor overall network performance is most likely the cause.

3. DECnet Vital Signs can be configured to include certain thresholds and to stop all measurements when a threshold is exceeded. From the DECnet Vital Signs window, select **[Config | Configure measurement]**.

4. Select **[Log threshold events]**. Page down to the NSP Retrans CI Threshold, set it for **[5]**, and check the **[Stop on Threshold]**. From the menu bar, select **[Done | Accept changes and exit]**. Re-run the DECnet Vital Signs from the capture buffer by selecting **[Control | Run Measurement From Capture Buffer | All Frames]**. The measurement will stop and display a message that it stopped due to the threshold being exceeded.



DECnet Vitals stopped by NSP retrans threshold

To investigate any DECnet Vital Sign events further, you should run the DECnet Commentator. It provides additional detailed information about any of the DECnet Phase IV or V events.

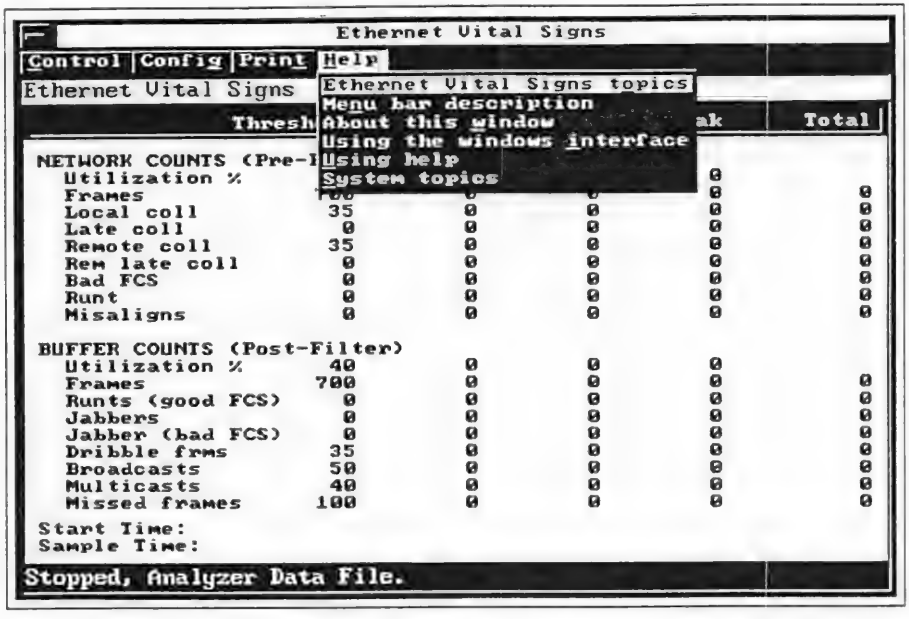
5. Press **[F5]** to close the DECnet Vital Signs measurement.

Help Text for Vital Signs

Vital Signs measurements contain a wealth of information about your network's physical layer activity and how your protocols are operating on the network. Often, it is not possible to remember what every field means. Context-sensitive help text is provided for your convenience. If you are not sure of the exact meaning of a field in a vitals measurement, simply click on the Help menu option to review the Help text.

1. From the Measurements window, Statistics category, select **[Ethernet Vital Signs]** and press **[Enter]**.

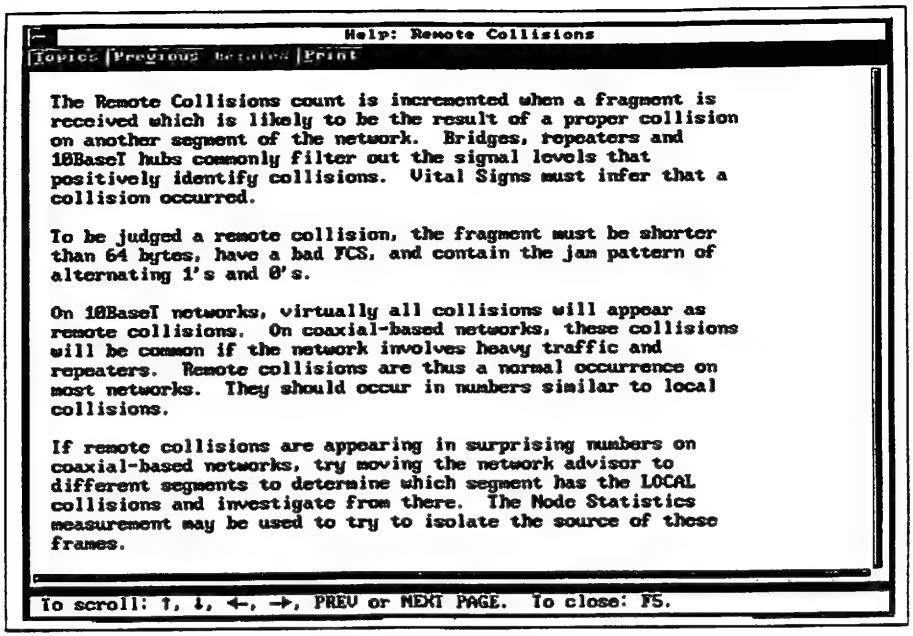
2. From the menu bar, select **[Help]**.



Context Sensitive Help text available in all measurements

3. Select **[Ethernet Vital Signs topics]**. From there, select the topic **[Remote Collisions]**. Press **[F4 | Z]** to zoom the window.

This context-sensitive Help text can be found in all measurements on the Internet Advisor.



Help text for Remote Collisions

4. Press **[F5]** to close the Help text window.
5. Press **[F5]** to close the Ethernet Vital Signs measurement.

Chapter Notes

Chapter 7 - Commentators

Objective

Isolating a LAN problem or tuning a network can often mean searching through thousands of captured frames, most of which are insignificant or irrelevant. Commentators will increase your productivity and save you time by automating the processing of this information and helping you determine what is important and what is not.

Think of Commentators as expert troubleshooters for monitoring data traffic, following the protocols, and reducing hundreds of frames to a handful of significant events. Each event is completely described, time-stamped, and rated in terms of its severity. Commentators operate in real time, interpreting data traffic as it occurs.

For a given media, you can run all protocol Commentators simultaneously from the Network Commentator, or you can select them individually Frame numbers causing the Commentator events are listed so that you can view specific frames to define and resolve the network problems.

In this chapter, you will learn to configure and run Commentators to better manage and troubleshoot your network, and you will also learn how to review individual frames with decodes.

Topics Covered

- Novell Commentator -- Observe and summarize a Novell client accessing a server
- TCP/IP Commentator-- Analyzing Telnet and FTP operations
- ICMP Commentator -- Analyzing a misconfigured node performing a FTP file transfer
- DECnet Commentator -- Analyzing normal, warning, and alert events
- Help text for Commentators

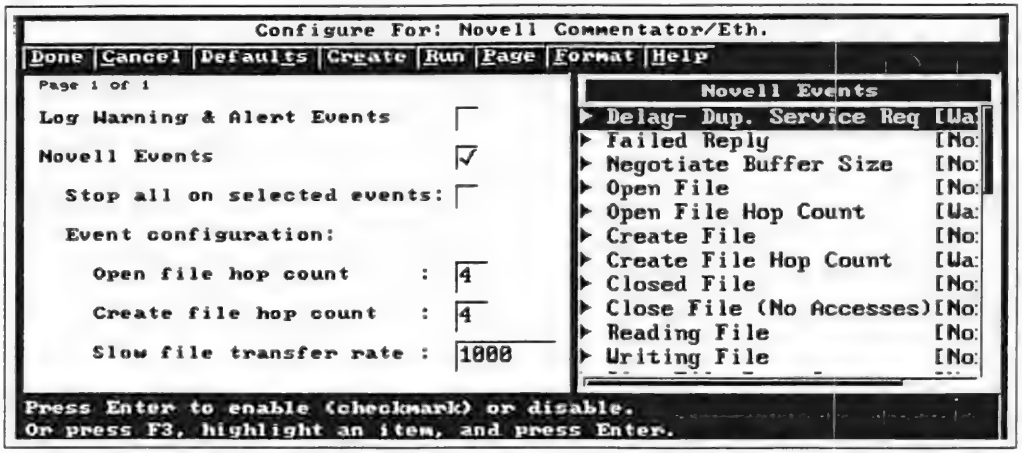
Preparation

- Internet Advisor for Ethernet should not have any measurements running.
- The Measurements window is properly sized, and the categories are fully expanded.
- The Node List **c:\user\class\class.lst** should be loaded.
- The Advisor Data File **c:\user\class\comm.eth** must be loaded into the capture buffer.

Run Novell Commentator

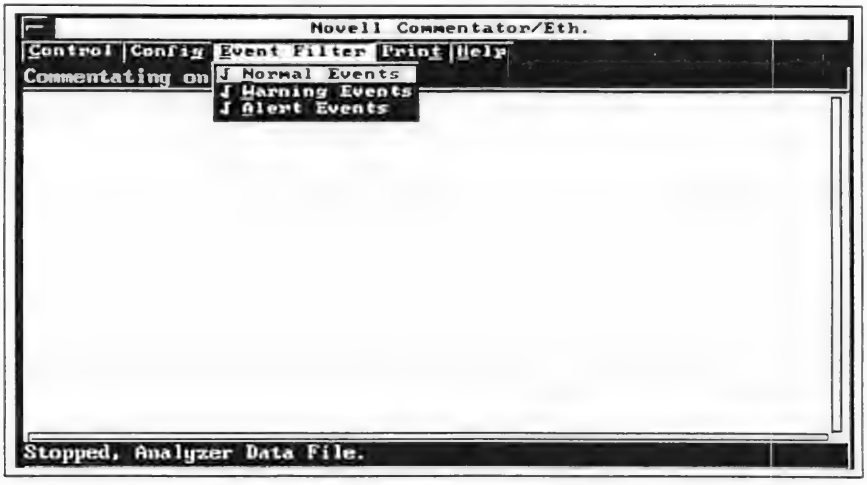
1. From the Measurements window, Commentators category, select **[Novell Commentator/Eth]** and press **[Enter]**.

2. Configure the Commentators. From the menu bar, select **[Config | Configure measurement]**. Select **[Defaults | Restore default values]**. Select **[Done | Accept changes and exit]**.



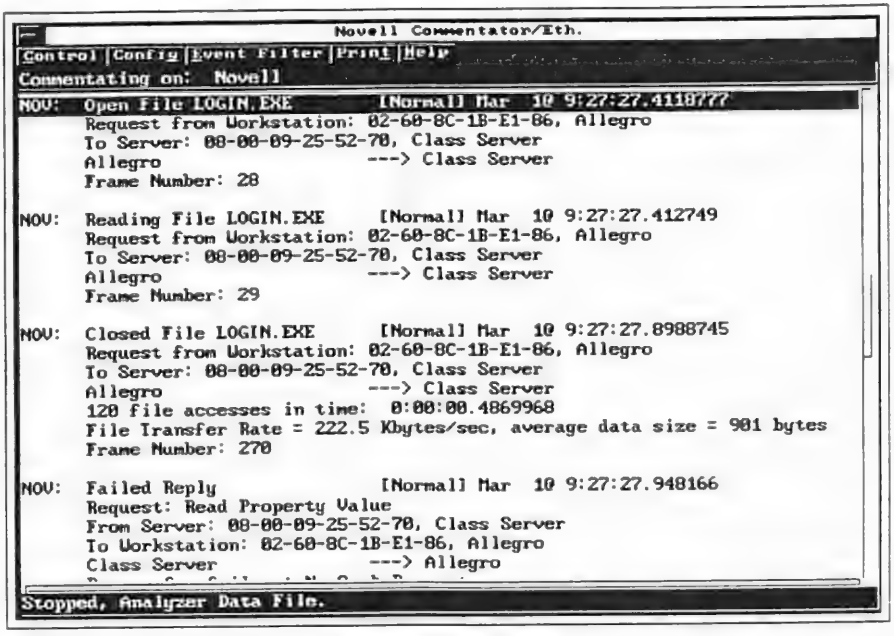
Novell Commentator configuration screen

3. From the Commentator's menu bar, select **[Event Filter]**. The Event Filter in the Network Commentator acts like a display filter. The actual network data is still captured by the Internet Advisor for Ethernet. Ensure that there is a check mark next to each event level in order to display Normal, Warning, and Alert events.



Normal, Warning, and Alert Events selected

4. Run the Network Commentator. From the menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**. Zoom the Commentator window **[F4 | Z]**, and press the **[Home]** key.



Novell Commentator window

Events Observed Using the COMM.ETH Advisor Data File:

Nearest Server Query/Response—The Service Advertising Protocol allows nodes that provide a service, for example, file or print servers, to advertise the service and their address. Workstations can request the name and address of the nearest server of a certain type, and they will receive a response from the server.

Routing Information—Request/Responses is used to exchange routing information. The request packet is used by workstations to find the fastest route to a remote node. The response contains a list of network numbers and the hops-away count to that network.

Negotiate Buffer Size—This event shows the transaction between the workstation and file server for negotiating the buffer size to be used in future transactions between the two. The buffer sizes should match and be as large as possible for a given configuration.

Failed Replies—These are normal and are viewed by Commentator as the client searches down through the file system on the class server. The amount of failed replies can be reduced by optimizing the file path structure on the server.

Open File LOGIN.EXE—Client requesting to open a file on the server.

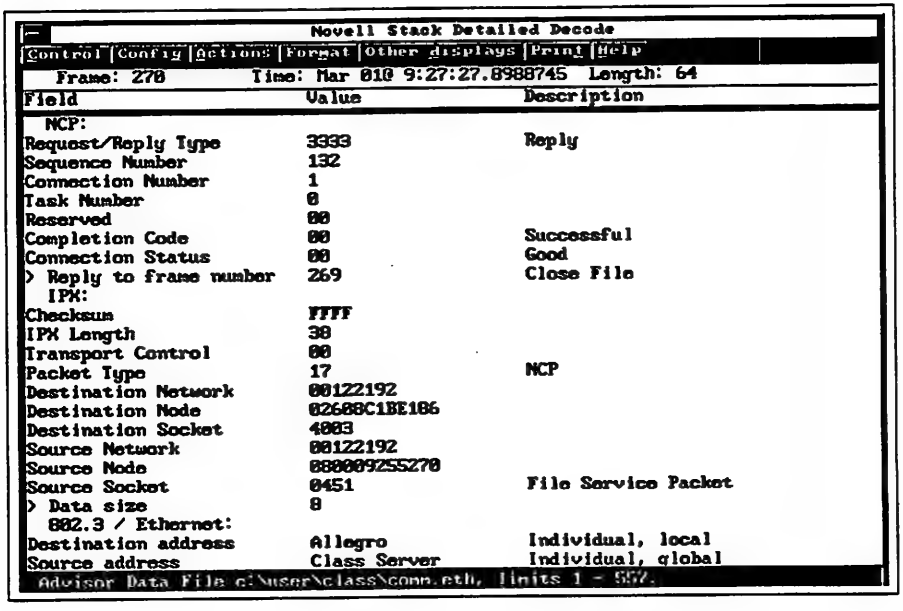
Reading File LOGIN.EXE—Client requesting to read a file on the server.

Closed File LOGIN.EXE—Specified file has been closed. The number of file accesses and the time taken (in hours, minutes, seconds, and fractions of seconds) for the file transfer are shown. It also shows the rate of transfer in kbytes/second, and the average data size of the packet.

5. Type **[open]** to find the first "open file" comment. Use the Shift key and Down Arrow key simultaneously to position the Commentator window as shown on the previous page. Notice the frame number for the "Closed File LOGIN.EXE" event, frame # 270.

6. Use the down arrow key to highlight the "**NOV: Closed File LOGIN.EXE**" comment description line and press **[Enter]**. The Help Text window opens and displays information about a Novell file close. After reviewing the help text, press **[F5]** to close the help text window.

7. Use the down arrow key to highlight the "**Frame Number: 270**" comment description line and press **[Enter]**. The Novell Stack Detailed Decode window opens and displays frame number 270. Press **[F4 | Z]** to zoom the window.



Novell Stack Detail Decode - frame 270 displayed.

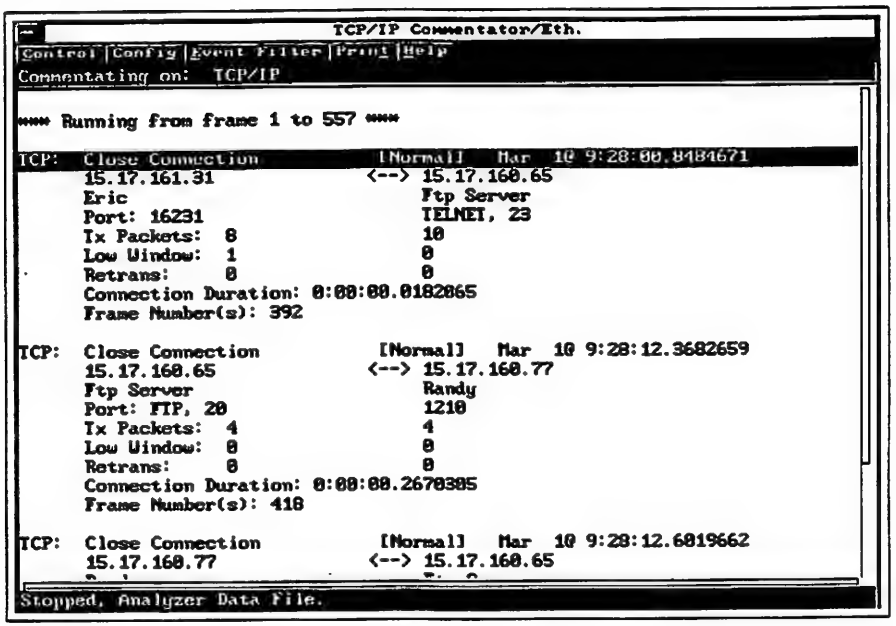
8. You can see that Commentator distills the important information from frames in the capture buffer, or on the network. Press **[F5]** to close the decode window and press **[F5]** to close the commentator window.

Run the TCP/IP Commentator

1. From the Measurements window, Commentators category, select the **[TCP/IP Commentator/Eth]** and press **[Enter]** to open the Commentator window.

2. From the menu bar, select **[Config | Configure measurement]**. Select **[Defaults | Restore default values]**. From the menu bar, select **[Done | Accept changes and exit]**.

3. Press **[F4 | Z]** to zoom the commentator window, then run the measurement from the capture buffer by selecting **[Control | Run Measurement From Capture Buffer | All Frames]**. Press the **[Home]** key.



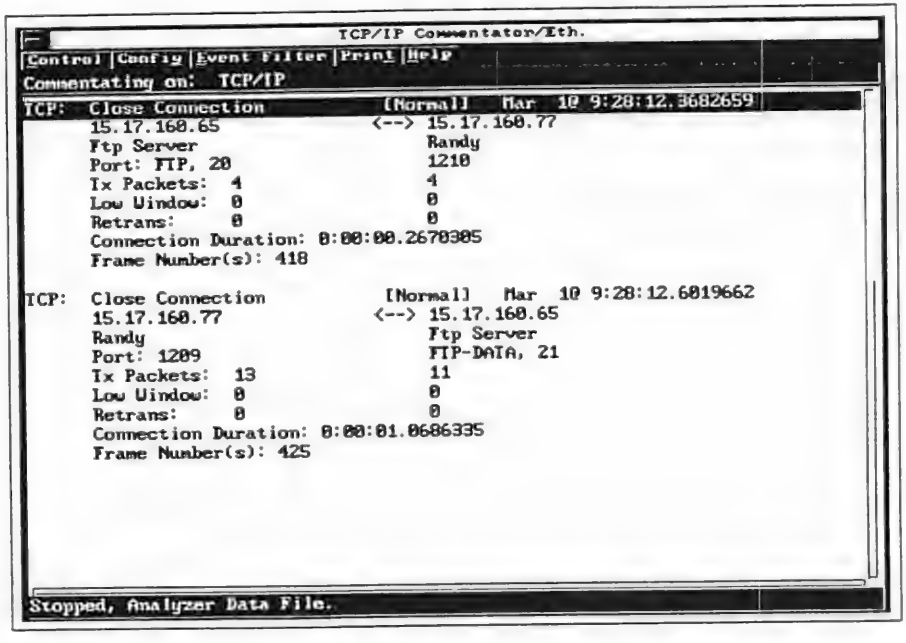
TCP/IP Commentator window

A single event, "TCP:Close Connection" occurs several times. Note the number of transmissions on each side of the connection. The Telnet application transmits many small packets, as viewed with the TX Packet count.

4. To view more details about Commentator events, select **[Help | Eth. Network Commentator topics]** from the menu bar. After reviewing the Help text press **[F5]** to close the Help text window.

Next, examine an FTP control connection and an FTP file transfer connection using the TCP/IP Commentator and the Advisor data file already re-played. In practice, this procedure works best if you create a level 2 hardware address filter to narrow down the frames to be analyzed. Although you are looking at a layer 3 Internet connection, it is best to use a hardware filter so that you can capture non-connection-oriented frames such as ARPs.

Both FTP and Telnet applications require the same overhead in setting up their TCP connections. FTP is complicated by this because it sets up two connections when an actual file is transferred: one control connection that transfers commands to/from the user (the **put** command tells the other FTP agent to prepare for a file transfer, etc.); and one data connection that carries the actual file data.



Two TCP Close Connections for FTP file transfer

Note the number of transmissions on each side of the two connections. FTP file transfer protocol sends fewer, but larger, packets as compared to the Telnet example on the previous page.

Two "TCP: Close Connection" events will occur. One event is for the FTP control connection; the other is for the FTP data (file transfer) connection.

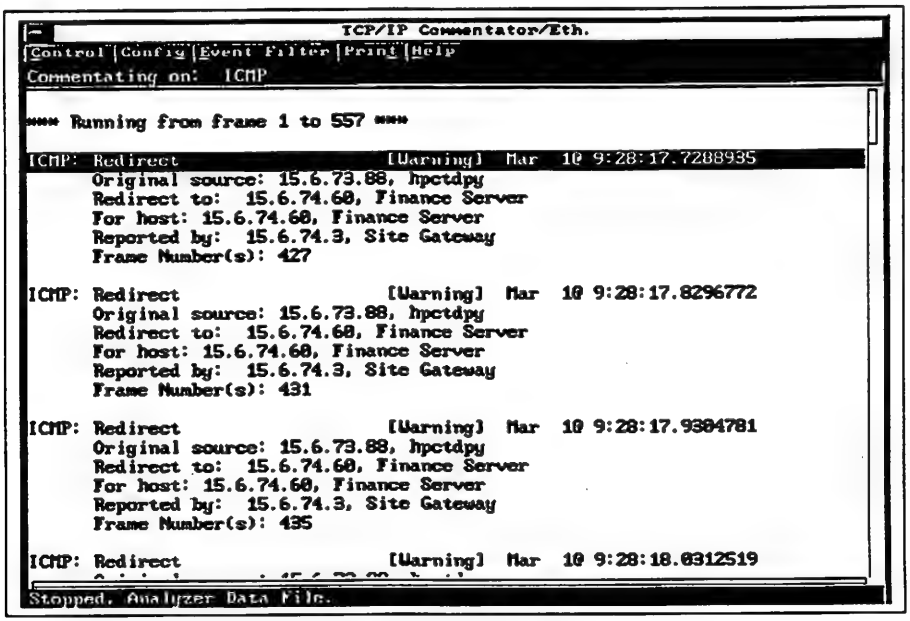
Run the ICMP Commentator

1. From the TCP/IP Commentator window, select **[Config | Configure measurement]**. The TCP/IP Events is currently selected.

2. Configure the measurement to observe just the ICMP protocol. Select **[Page | Next page]** and put a check mark in the **[ICMP Events]** field. Select **[Page | Previous page]** and de-select the **[TCP/IP Events]** field by ensuring that no check mark appears in that field. At least one category must be selected at all times or the Advisor will produce a warning beep. From the menu bar, select **[Done | Accept changes and exit]**.

3. From the menu bar, select **[Control | Run Measurement From Capture Buffer | All Frames]**. Press the **[Home]** key to observe the first events.

The ICMP event displays a host redirect, which means that an intermediate node is redirecting the originating node's frame. Notice that for each frame hpctdpy sends, the site gateway, whose address is 15.6.74.3, must redirect the frame to the finance server which is on the same network as hpctdpy. This indicates a misconfigured IP subnet mask.



TCP/IP Commentator with ICMP comments

The problem here is that hpctdpy moved from another department and the LAN Administrator overlooked assigning it a new subnet address. Hpctdpy previously resided on a .73 subnet, and now it is assigned to a .74 subnet.

4. Press **[F5]** to close the Commentator measurement.

Run DECnet Commentators

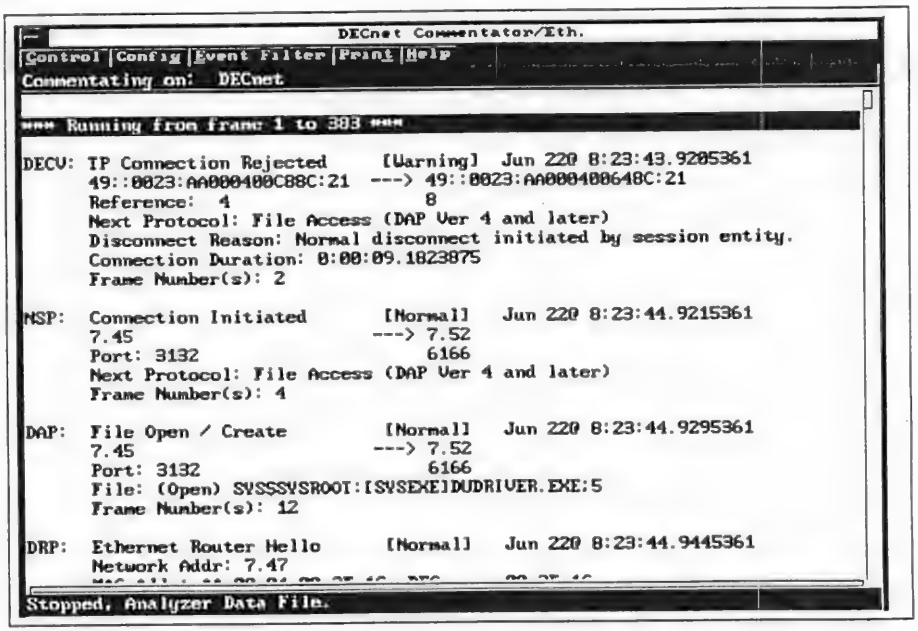
Run the DECnet Commentator and review a normal event, a warning event, and an alert event. The Advisor Data File **c:\user\class\decnet.eth** must be loaded into the capture buffer.

NOTE: The data contained in the decnet.eth data file was created in a lab environment. Actual DECnet data may be different. This file was created to trigger all the DECnet Commentator events.

1. From the Measurements window, Commentators category, select **[DECnet Commentator/Eth]** and press **[Enter]** to open the measurement.

2. Configure the Commentator. From the menu bar, select **[Config | Configure measurement]**. Select **[Defaults | Restore default values]** then select **[Done | Accept changes and exit]**.

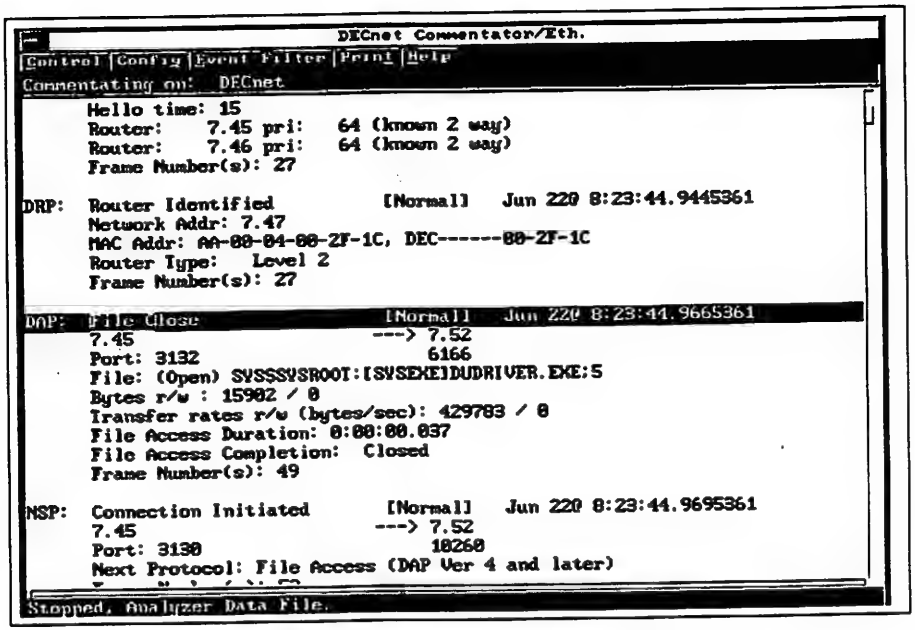
3. Run Commentator from the capture buffer by selecting **[Control | Run Measurement From Capture Buffer | All Frames]**, then press **[F4 | Z]** to zoom the commentator window, and press the **[Home]** key.



DECnet Commentator window

The DECnet Commentator measurement provides a high-level view of significant network events. These events may signal problems that could lead to network performance degradation or network failure. DECnet Commentator lets you identify potential network problems without sifting through pages of decodes. The DECnet Commentator provides detailed information about DECnet Phase IV and V events.

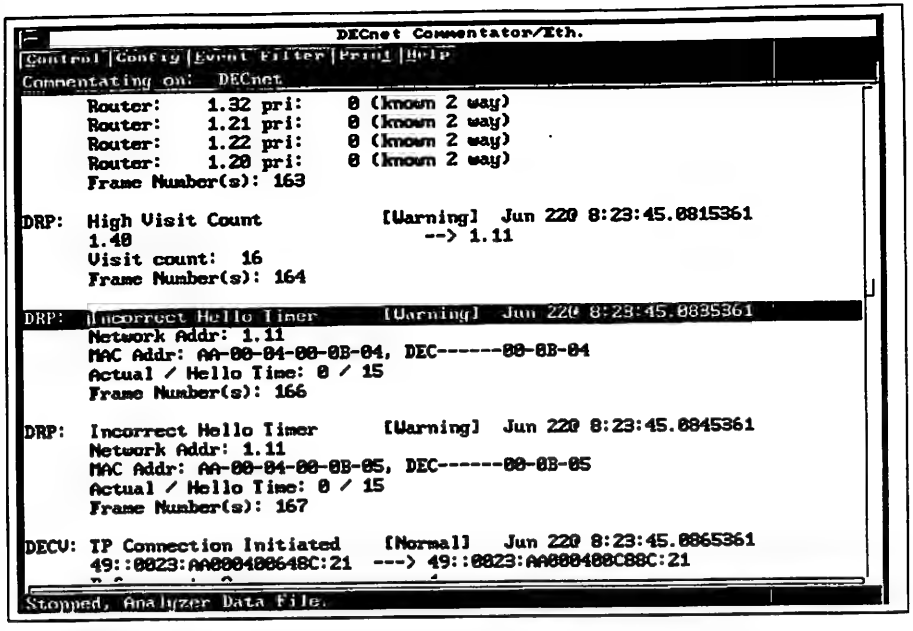
4. First, review a Normal DECnet event -- a file close. To find the file close comment quickly, type **[file close]**, and notice that the DAP: File Close comment appears on the screen.



First file close comment

The File Close comment provides information about which nodes were involved, which file was closed, and file transfer rates. The Commentator provides all details necessary to troubleshoot without using decodes. However, if you want to review the data using a decode, then use the down arrow key to highlight the "**Frame Number(s): 49**" comment description line and press **[Enter]**. The DECnet IV & V Stack Detailed Decode opens and displays frame 49.

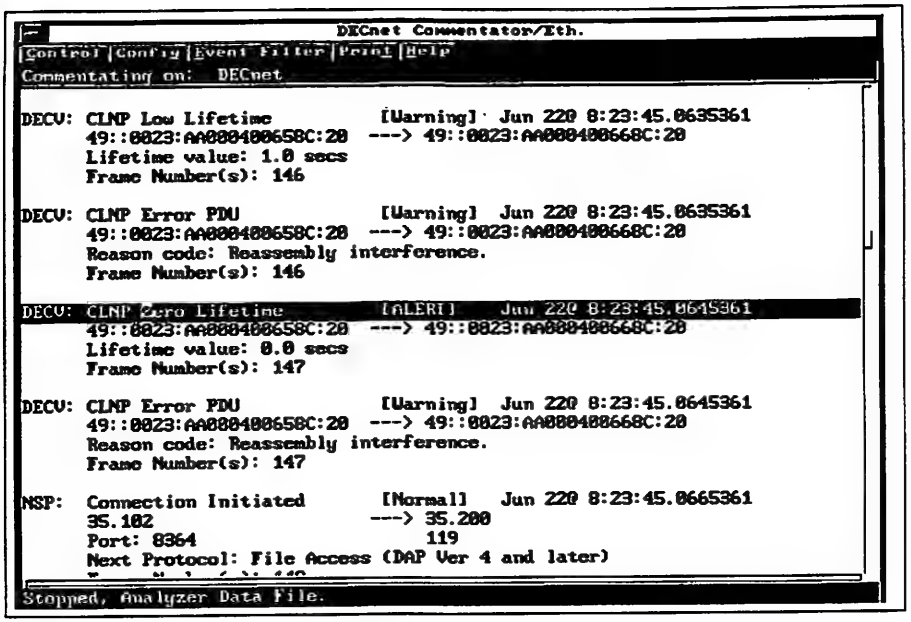
5. Next review a Warning event -- a DRP Incorrect Hello Timer. To find this event, press **[CTRL]** and **[E]** simultaneously, to erase the last search then, type **[incorrect]**, and the first "incorrect hello timer" comment is displayed. To find additional incorrect hello timer comments, press **[CTRL]** and **[F]** simultaneously. To search backward, press **[CTRL]** and **[B]** simultaneously.



First Incorrect Hello Timer comment

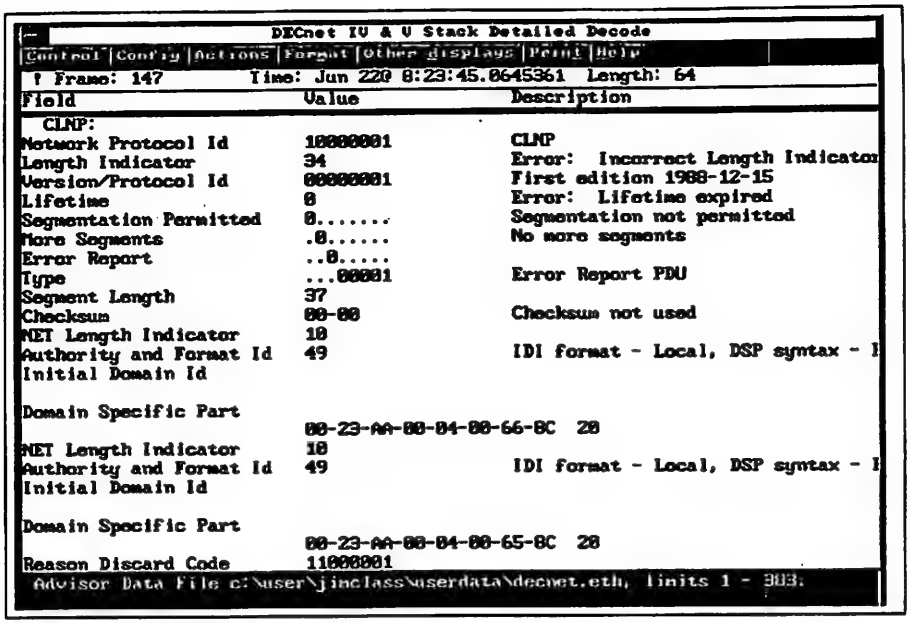
An Incorrect Hello Timer event is triggered if the actual time interval between two Endnode Hello messages is less than or greater than the Hello Timer field in the frame by N seconds. N is specified on the Commentator configuration page in the Hello Time Threshold field of the DECnet events. Since DECnet is a chatty protocol, you will want to ensure that individual nodes are not sending Hello messages too often.

6. Finally, review an Alert event -- CLNP Zero Lifetime. To find this event, press **[CTRL]** and **[E]** simultaneously, to erase the last search then, type **[zero]**, and the first "zero lifetime" comment is displayed. A zero lifetime frame means that the frame cannot be forwarded to another network segment. Depending upon where you are monitoring the network, a zero lifetime frame can indicate serious problems. If a frame is dropped because there is a zero lifetime, and that frame needed to go to another segment to communicate with the server, then the network performance is not optimum due to requests for retransmissions.



First CLNP zero lifetime comment

7. A closer look at this frame with the DECnet IV & V Stack Decode shows that the field lifetime is set at zero. Use the down arrow key to highlight the "**Frame Number(s): 147**" comment description line, and press **[Enter]**. The DECnet IV & V Stack Decode opens and displays frame 147. Press **[F4 | Z]** to zoom the decode window.



DECnet Stack Detailed Decode with frame 147 displayed

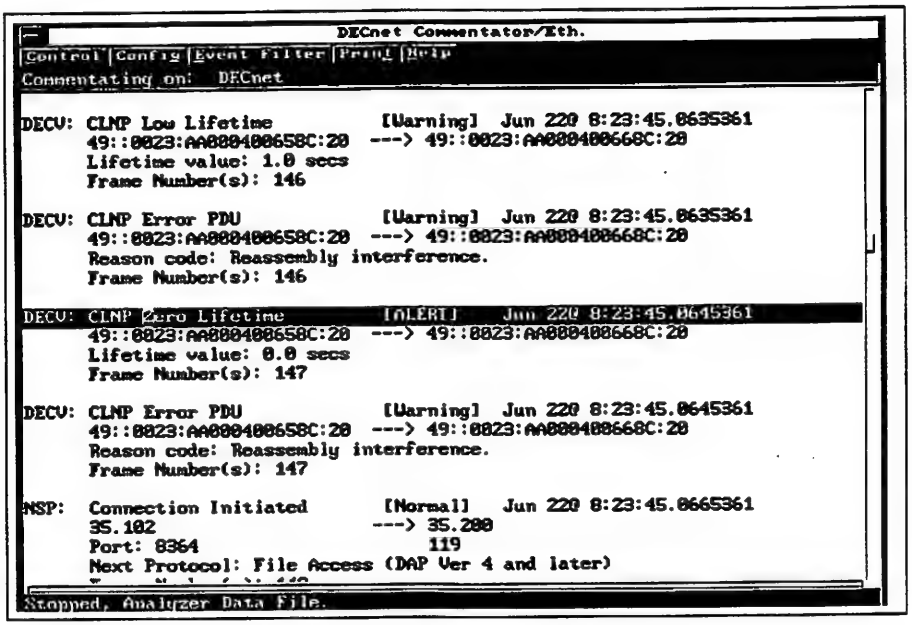
Note the frame is identified (an exclamation mark next to the frame number) as an error. Two errors are reported. One is incorrect length due to our generation of the test frame. The second error is the lifetime expired error.

8. Press **[F5]** to close the decode window. Do not close the DECnet Commentator.

Help Text for Commentators

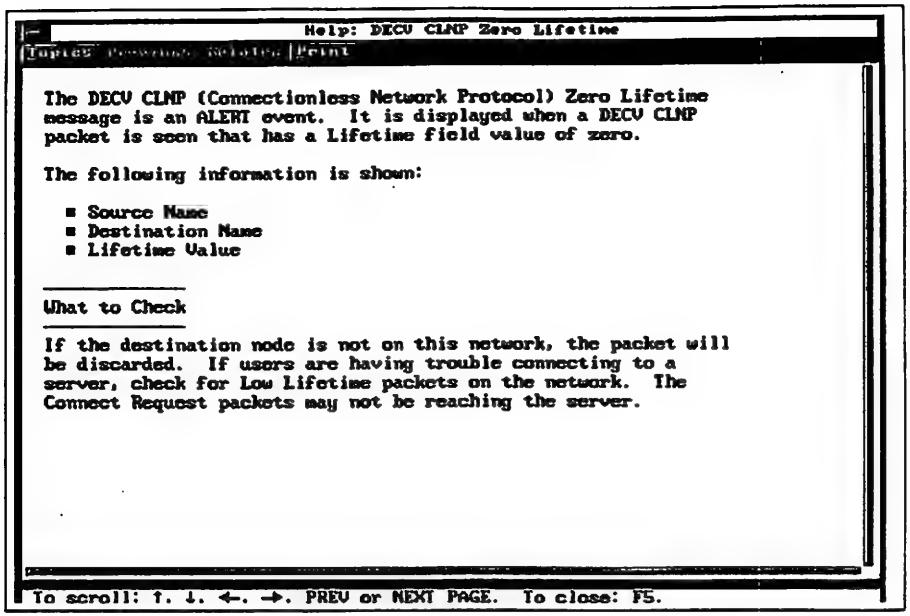
A wealth of information is provided in the Commentators. Since it is not always possible to remember exactly what each comment means, context-sensitive Help has been provided within the Commentator measurement.

1. If you need assistance in understanding a comment, from any Commentator's comment description line, press enter and the Help text window appears with a detailed description of that comment. For example: Use your down arrow, or up arrow key to highlight a comment description line, in this case, highlight the **"DECV: CLNP Zero Lifetime"** comment description line and press **[Enter]**.



DECV: CLNP Zero Lifetime comment description line

The Help text window appears with a detailed description of the CLNP Zero Lifetime comment. Press **[F4 | Z]** to zoom the Help text window.



Help text for DECV CLNP Zero Lifetime

Detailed Help text can be viewed from the Commentator measurements or any other Internet Advisor for Ethernet measurement.

4. Close the Help text window by pressing **[F5]**.

5. Press **[F5]** to close the Commentator window.

Chapter Notes

Chapter Notes

Chapter 8 - Traffic Generator

Objective

The traffic generator in the Internet Advisor for Ethernet allows you to transmit messages (frames) onto the network. By generating traffic and then making measurements, you can recreate and analyze network problems that are related to traffic level.

You can test a node or network to determine the limits of network hardware or protocol implementations by either increasing the amount of traffic it handles, or by inducing perturbations on the network. The traffic generator also lets you find the limits of a device or a group of nodes for handling congestion or errors.

A maximum of 32 types of messages are available so that you can duplicate nearly any kind of traffic. Frames that were previously captured into the buffer can also be copied into any or all of these 32 messages to duplicate previously captured data, or to aid in creating complex messages.

For stress testing applications, you can specify the traffic load in these ways:

- percent utilization
- frames per second
- inter-frame spacing

You can also create errored frames to evaluate a network's sensitivity to errors.

Topics Covered

- Examining Traffic Generator functionality
- Create a Traffic Generator measurement
- Delete a Traffic Generator measurement

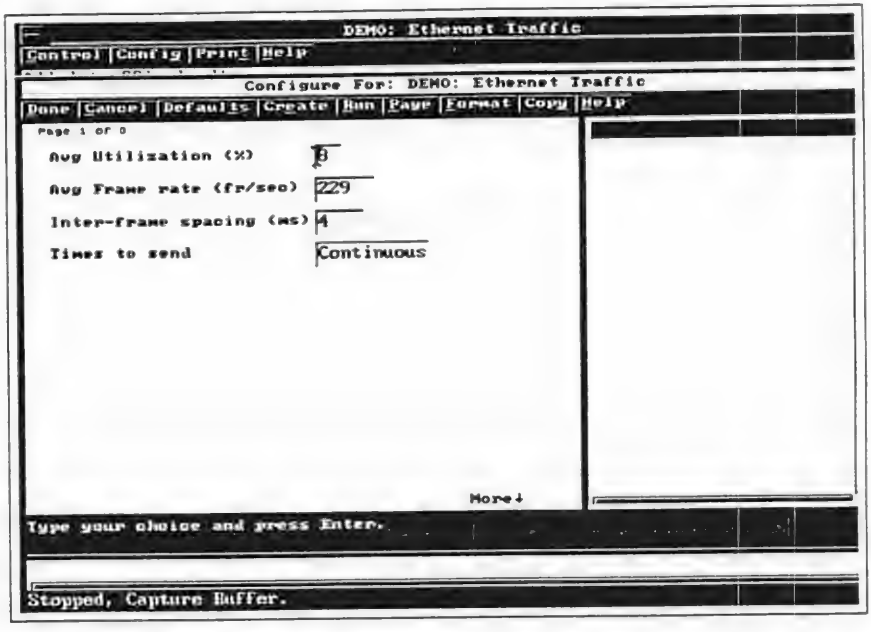
Preparation

- Internet Advisor for Ethernet should not have any measurements running.
- The Measurements window is properly sized and the categories are fully expanded.

Examine Traffic Generator Functionality

1. From the Measurements window, Demo Tools category, select the **[Demo: Ethernet Traffic]**. From the Measurements window menu bar, select **[Control | Open selected measurements]**. Press **[F4 | Z]** to zoom the DEMO: Ethernet Traffic window.

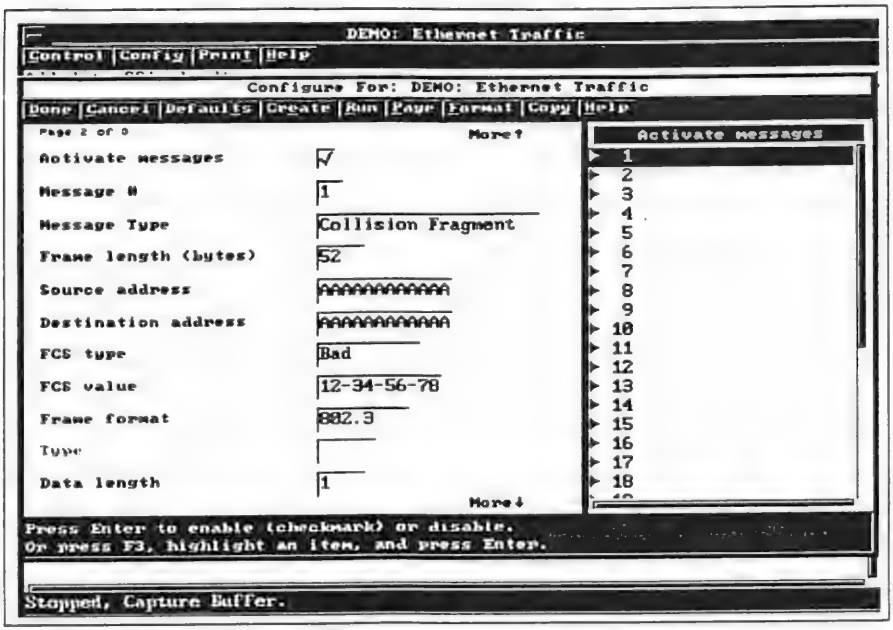
2. From the DEMO: Ethernet Traffic window menu bar, select **[Config | Configure measurement]**.



DEMO: Ethernet Traffic measurement – first configuration screen.

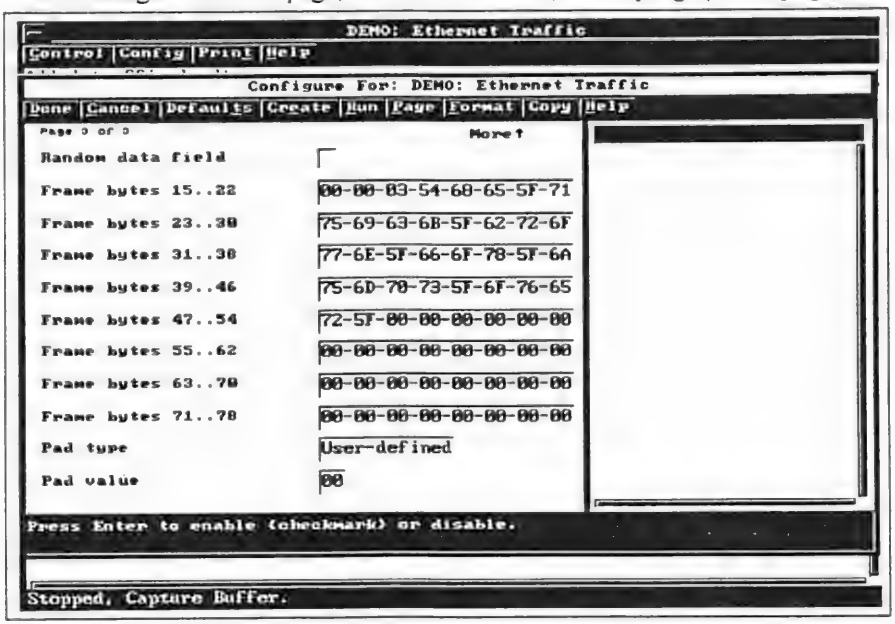
Three pages of configuration items can be found in the configuration window.

3. To view the settings on the next page, select **[Page | Next page]** from the menu bar. When another page is available, you'll see "**More**" at the bottom of the current configuration window.



DEMO: Ethernet Traffic measurement – second configuration window.

4. To view the settings on the last page, from the menu bar, select **[Page | Next page]**.



DEMO: Ethernet Traffic measurement – third configuration window.

Fields contained in the first two pages of the configuration window are described below:

Page 1 Settings	Function
Avg Utilization (%)	Displays the average percentage of the network's capacity that will be used under the current traffic load conditions.
Avg Frame rate (fr/sec)	Lets you specify the average number of frames that will be transmitted per second under the current traffic load conditions.
Inter-frame spacing (ms)	Specifies the amount of time, in milliseconds, between frames under the current traffic load conditions.
Times to send	Specifies how many times the Internet Advisor for Ethernet is to send the currently activated frame(s).
Page 2 Settings	**Function**
Activate messages	Lets you enable the messages you want to transmit when you run the measurement.
Message #	Lets you select any of the available messages to edit.
Message Type	Lets you choose from a selection of predefined messages or enter a message name of your choice.
Frame length (bytes)	Specifies how many bytes, including the FCS, the frame contains. When modified, the values for Avg Frame rate and Avg Utilization are automatically calculated and updated.
Source address	Specifies the source address of the frame (either a hex value, or a node name in the Internet Advisor for Ethernet 's node list).
Destination address	Specifies the destination address of the frame (either a hex value, or a node name in the Internet Advisor for Ethernet's node list).
FCS type	Lets you specify whether the frame will have a good or bad Frame Check Sequence.
FCS value	Indicates the FCS value when the FCS type field is set to have a bad FCS. Otherwise (if the frame will have a good FCS) this field is disabled.
Frame format	Lets you control whether the format of the message is Ethernet or 802.3. Then you can select the Ethernet frame type field or the 802.3 data length field accordingly.
Type	When the Frame format field is Ethernet, this indicates the types of predetermined Ethernet frames that you can select. When the Frame format field is 802.3, this field is disabled.
Data length	When the Frame format field is 802.3, this lets you change the number of bytes in the data field that will be transmitted with the current frame. When the Frame format field is Ethernet, this field is disabled.

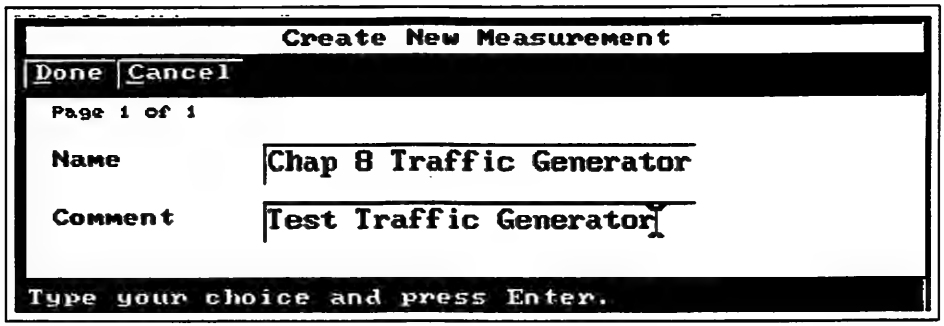
5. Close the DEMO: Ethernet Traffic measurement without making any permanent changes to it. From the menu bar, select **[Cancel | Cancel changes and exit]**. Close the measurement by pressing **[F5]**.

Create a Traffic Generator Measurement

You can create and save multiple traffic generator measurements, which allows you the flexibility to create custom traffic generator measurements for stress testing networks or components. You don't have to change the configuration every time you want to use the traffic generator for a different purpose.

1. From the Measurements window, Stimulus/Response Test category, select the **[Eth. Traffic Generator]**. From the Measurements window menu bar, select **[Control | Open selected measurements]**.

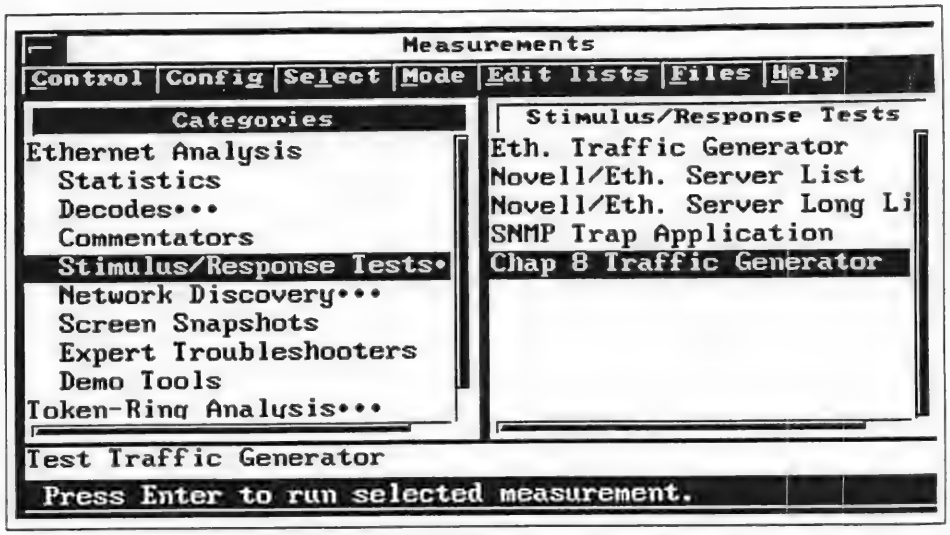
2. From the Eth. Traffic Generator menu bar, select **[Config | Configure measurement]**. From the menu bar, select **[Create | Create new measurement]**. Name the measurement **[Chap 8 Traffic Generator]** and add **[Test Traffic Generator]** to the Comment field. From the menu bar, select **[Done | Accept changes and exit]**.



Creating new traffic generator measurement

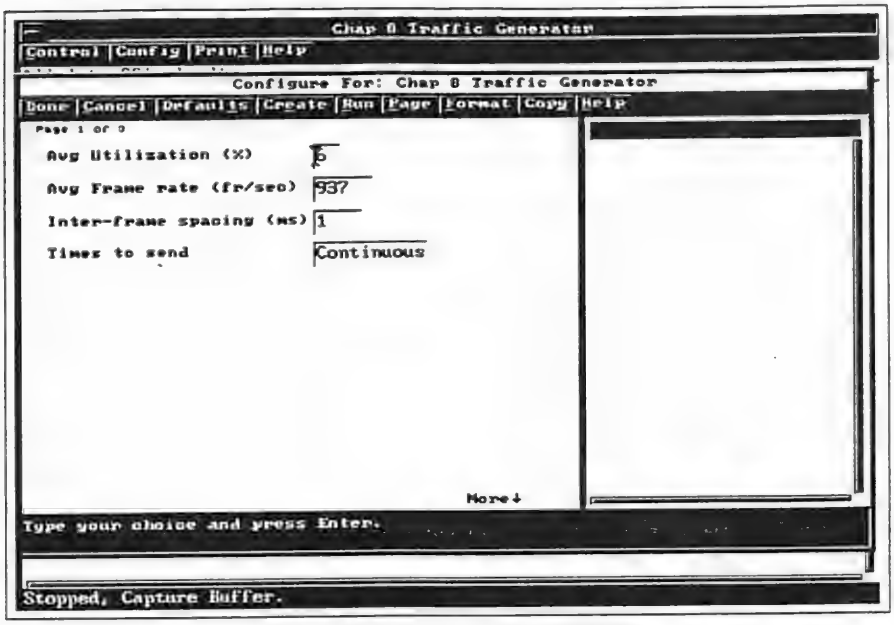
3. From the Eth. Traffic Generator window, select **[Cancel | Cancel changes and exit]**. This ensures that the original traffic generator measurement does not change. Press **[F5]** to close the Eth. Traffic Generator measurement.

The Measurements window shows the new "Chap 8 Traffic Generator" measurement in the Stimulus/Response Tests pane.



New traffic generator measurement available in Stimulus/Response Tests

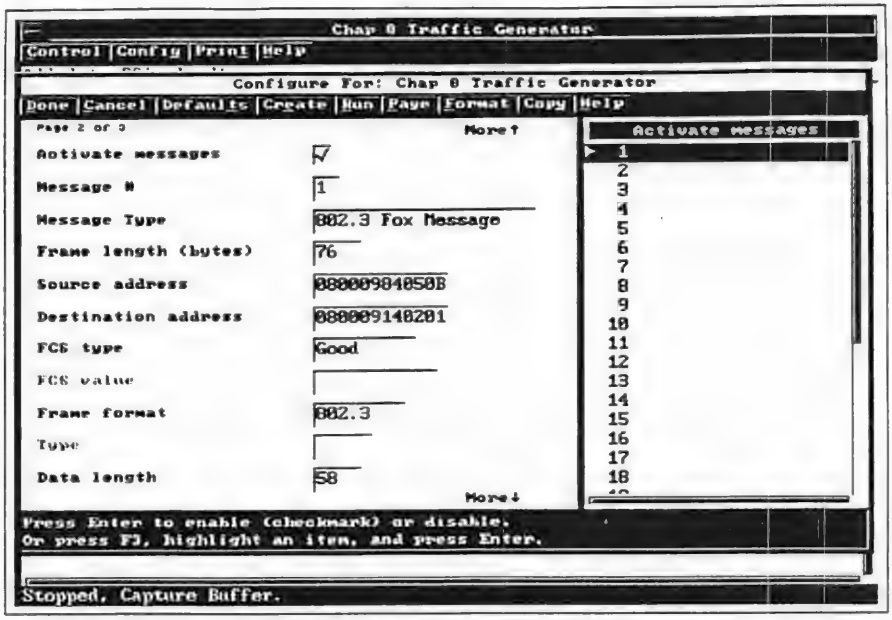
4. From the Measurements window, Stimulus/Response Tests, select **[Chap 8 Traffic Generator]**. From the Measurements window menu bar, select **[Control | Open selected measurements]**. Press **[F4 | Z]** to zoom the window. From the menu bar, select **[Config | Configure measurement]**.



Chap 8 Traffic Generator main configuration window

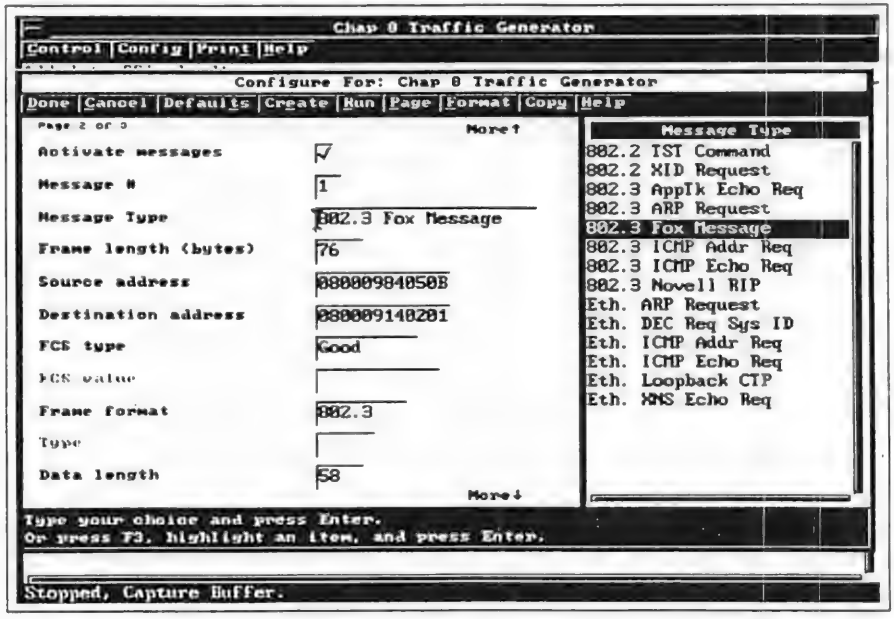
In this configuration window, you can select: Average Utilization percent to send; Average Frame rate (in frames per second); Inter-frame spacing; and the Times to send, either continuous, or a number of times per second.

5. The first 3 fields of this configuration page are interdependent. Change the "Avg Utilization (%)" field to **[10%]**. Note the change in Avg Frame rate. Change the "Avg Frame rate" field to **[3000]**. Note the change to Avg Utilization field. Set "Avg Utilization (%)" to **[1%]**, then from the menu bar, select **[Page | Next page]**.



Chap 8 Traffic Generator, second configuration window

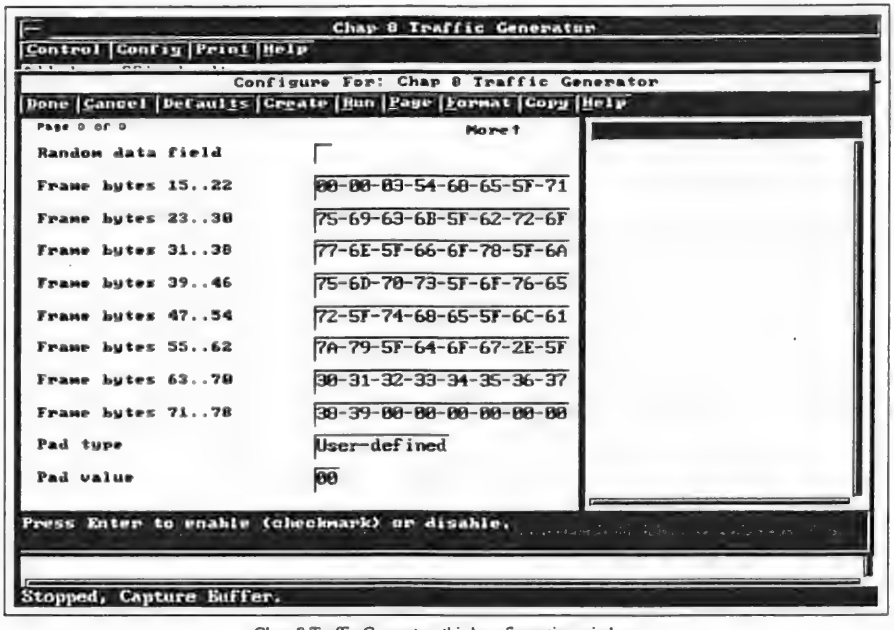
6. The Activate messages field shows there is only one message activated. You can activate up to 32 messages at a time. Messages are toggled on and off by selecting the message number in the Activate messages pane. The Message Type field is 802.3 Fox Message. Click on the Message Type field and note the pre-made message types available in the Message Type pane.



Multiple message types available

You can use one of these pre-made messages to send, you can create your own message, or you can copy a frame from the capture buffer (traffic generator menu bar, select [Copy | Copy from buffer | Frame #]).

7. The Source and Destination addresses, the FCS value, Frame format, and Data Length fields can be modified. Leave message 1, the fox message, activated. From the menu bar, select **[Page | Next page]**.



Chap 8 Traffic Generator, third configuration window

Frame bytes 15 - 78 can be customized. Byte 15 starts immediately after the Source Address in the Ethernet/802.3 frame. For bytes 79 - nnn (configured data length), padding is used (normally all 0s). Notice that the hex values for the fox message are loaded.

8. From the menu bar, select **[Done | Accept changes and exit]**. Your custom traffic generator measurement is ready to run. Caution: You may want to run this measurement with a loopback connector. If you elect to run it on your network, ensure that utilization is set to 1 percent and only one fox message will be sent.

9. From the menu bar, select **[Control | Run measurement]**. The traffic generator is password protected. If you are prompted for a password, the default set at the factory is "**advisor**". You can also run other measurements to monitor the impact of the traffic generator on your network. The Advisor is a multi-tasking instrument, so you can send traffic and analyze the network simultaneously.

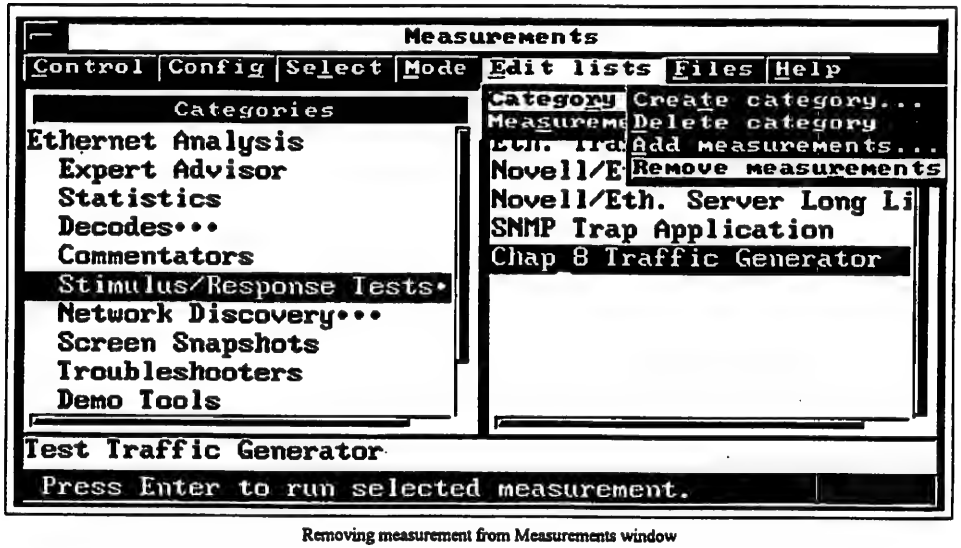
10. From the menu bar, select **[Control | Stop measurement]**. Press **[F5]** to close the measurement.

Delete a Traffic Generator Measurement

If you should have to remove a traffic generator measurement from the Stimulus/Response Tests category, follow the numbered instructions below. Also, be sure to remove the Chap 8 Traffic Generator measurement now.

1. From the Measurements window, Stimulus/Response Tests category, select the **[Chap 8 Traffic Generator]** measurement.

2. From the Measurements window menu bar, select **[Edit lists | Measurements | Remove measurement]**. A warning message will appear indicating you are deleting a measurement. Check whether you are deleting the proper one, and select **[yes]** and press **[Enter]**. Chap 8 Traffic Generator is removed from the Stimulus/Response Tests category.



Removing measurement from Measurements window

Chapter Notes

Chapter Notes

Chapter 9 - Stimulus Response Tests

Objective

Some network faults can be isolated using active stimulus/response testing—actively communicating with devices on the network. For example, observing Ethernet frames with the same IP address and different MAC addresses might indicate a duplicate IP address problem, or it might just result from a complex router topology. By ARPing the stations for their addresses, you can find out quickly.

The ARP (Address Resolution Protocol) Request test lets you check the hardware address of any node for which you know the IP address. Given the IP address of a node, this measurement returns that node's physical address.

The PING test verifies whether a route exists to any given IP address. The Internet Advisor sends an ICMP Echo Request and then filters for an ICMP Echo Reply from the target node.

The Stimulus/Response Tests category in the Internet Advisor for Ethernet contains measurements to actively test TCP/IP, and Novell nodes. This chapter will discuss these tests in detail so you can use them to become more efficient when troubleshooting your network or network nodes.

This chapter requires a live network for running the tests. If you don't have access to a live network, review this chapter for information only.

Topics Covered

- Running the ARP test
- Running the PING test
- Evaluating Novell tests
- Ethernet Transceiver test to verify proper operation of MAUs

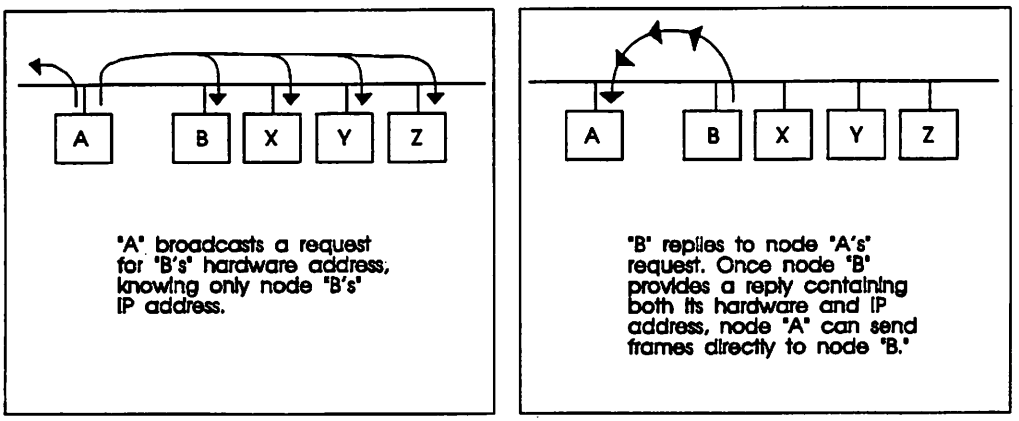
Preparation

- Internet Advisor for Ethernet should not have any measurements running.
- The Measurements window is properly sized and the categories are fully expanded.
- Access to a live network with Novell and/or TCP/IP nodes.

ARP Tests

ARP is an Internet standard for dynamic address binding. ARP does not guarantee the actual reachability or connectivity of a node. Usually a router or gateway will be configured to reply to ARP requests for nodes not on the subnet. This operation is known as a device running proxy ARP.

The ARP and PING tests transmit frames on the network and are therefore password protected. They also invoke automatic filters for the responses from their targets. These measurements perform optimally if no other measurements are running.



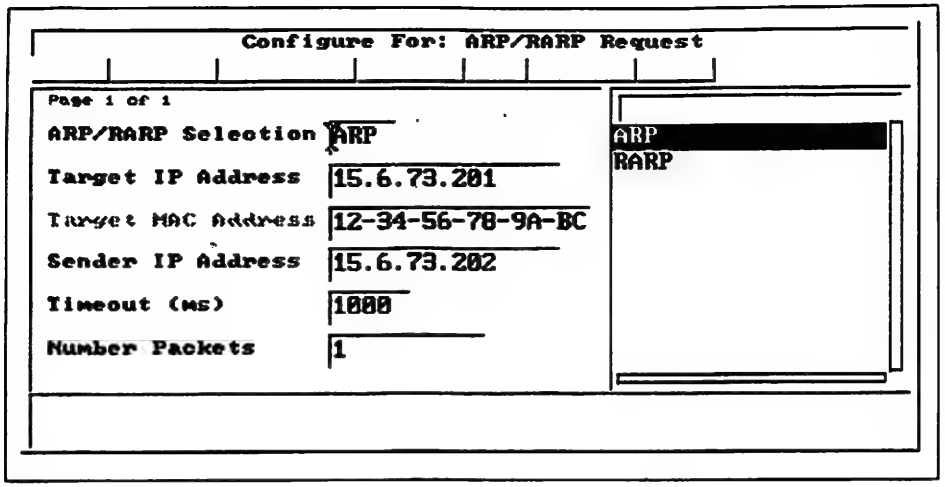
Example of how an ARP request works

1. From the Measurements window, select the **[Stimulus/Response Tests]** category and press **[Enter]** to expand the category to show Ethernet, Novell, and TCP/IP categories. Select the **[TCP/IP]** category.

2. Two measurements are available; ARP/RARP Request and PING. Select **[ARP/RARP Request]** and from the Measurements window menu bar, select **[Control | Open selected measurements]**. Press **[F4 | Z]** to zoom the ARP/RARP Request window.

3. From the menu bar, select **[Config | Configure measurement]**. Then:

Set the ARP/RARP field to **[ARP]**.
Set the Target IP Address field to **[nnn.nnn.nnn.nnn]** where nnn is the target IP host address.
Set the Sender IP Address field to **[nnn.nnn.nnn.nnn]** where nnn is a valid IP address.
Set the Number Packets field to **[3]**.

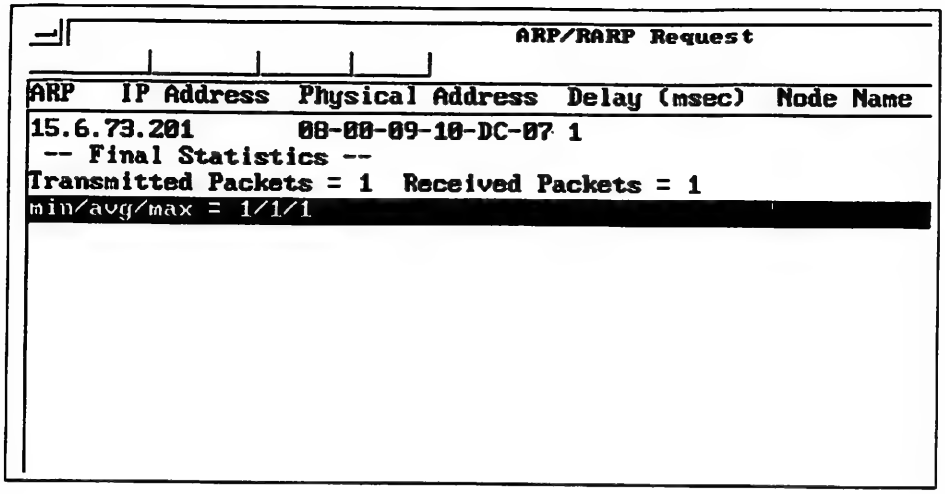


Configuration window for ARP/RARP Request

4. After filling in the fields, from the menu bar, select **[Done | Accept changes and exit]**. From the ARP/RARP Request window menu bar, select **[Control | Run measurement from network]**.

5. The Internet Advisor requires a password to transmit a frame onto the network. The Advisor password is case sensitive. The password is all lower case. Type **[advisor]** and press **[Enter]**. Note: The Filter status icon is active while the measurement is running. The Measurements Running status icon is red, indicating that a measurement is running and transmitting a frame or frames.

The example on the following page displays the results from the ARP request. Your results should look similar; however, the IP addresses will be different and the delay (msec) along with the min/avg/max response time should be different.



Results from running the ARP/RARP Request

6. Close the ARP/RARP Request measurement by pressing **[F5]**.

Note: In the ARP/RARP Request configuration window, from the menu bar, Create | Create new measurement is available. You can create multiple copies of the ARP/RARP measurement with custom configurations to test special nodes on your network. This saves the time of re-configuring the measurement before running it.

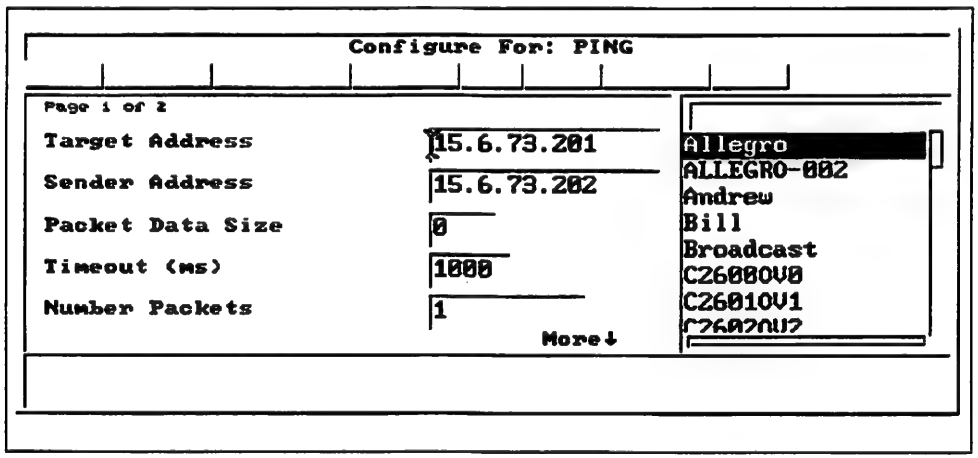
PING Test

PING is a test to verify whether a node can actually reach and communicate with a distant node. The target IP address must respond with a specific ICMP response. The PING uses the ICMP echo request frame to reach the target IP address. The target then must respond with an ICMP echo reply to the sender's IP address.

1. From the Measurements window, select the Stimulus/Response Tests category and press **[Enter]** to fully expand the category to show Ethernet, Novell, and TCP/IP tests. From the TCP/IP category, select **[PING]**, and from the Measurements window menu bar, select **[Control | Open selected measurements]**. Press **[F4 | Z]** to zoom the PING window.

2. From the menu bar, select **[Config | Configure measurement]**. Then:

Set the Target Address field to **[nnn.nnn.nnn.nnn]** where nnn is the IP address of the node you wish to reach. Set the Sender Address field to **[nnn.nnn.nnn.nnn]** where nnn is a valid IP address. Set the Packet Data Size field to **[0]**. Set the Timeout field to **[1000]**. Set the Number Packets field to **[3]**.



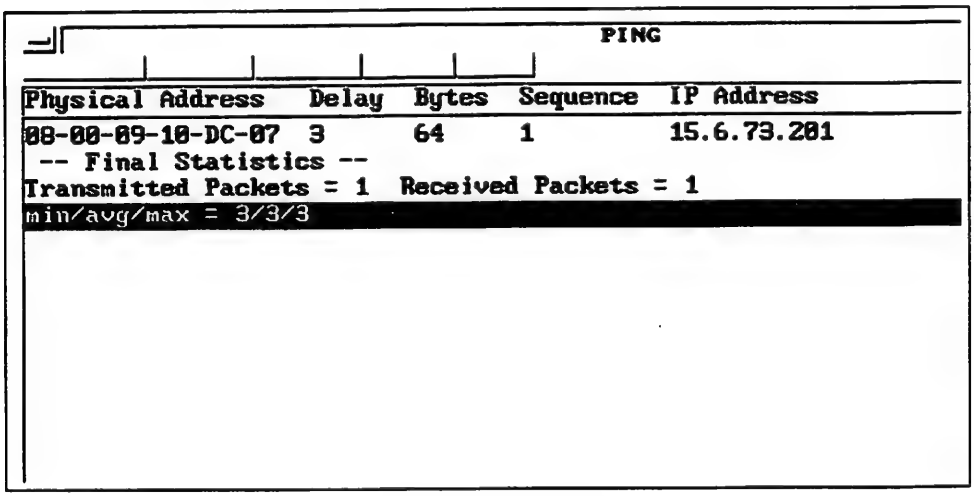
PING measurement configuration window

3. After you complete the first page of the PING configuration, use the Page Down key or from the menu bar select **[Page | Next page]** to see the second configuration page. This page contains the Default Router address and a selection box to enable default routing. Default routing is used when the target node is on the other side of a router or gateway. The IP address of that router or gateway must be entered here, and default routing must be enabled to successfully PING a node not on the local segment.

4. From the PING configuration window, select **[Done | Accept changes and exit]**. From the PING window menu bar, select **[Control | Run measurement]**.

5. The Advisor requires a password to transmit a frame onto the network. The Advisor password is case sensitive. The password is all lower case. Type **[advisor]** and press **[Enter]**. Note: The Filter status icon becomes active for a moment, and the Measurements Running status icon is red, indicating a measurement is running, and transmitting a frame or frames.

The following example displays the results from the PING measurement. Your results should look similar, however, the IP addresses will be different and the delay should be different.



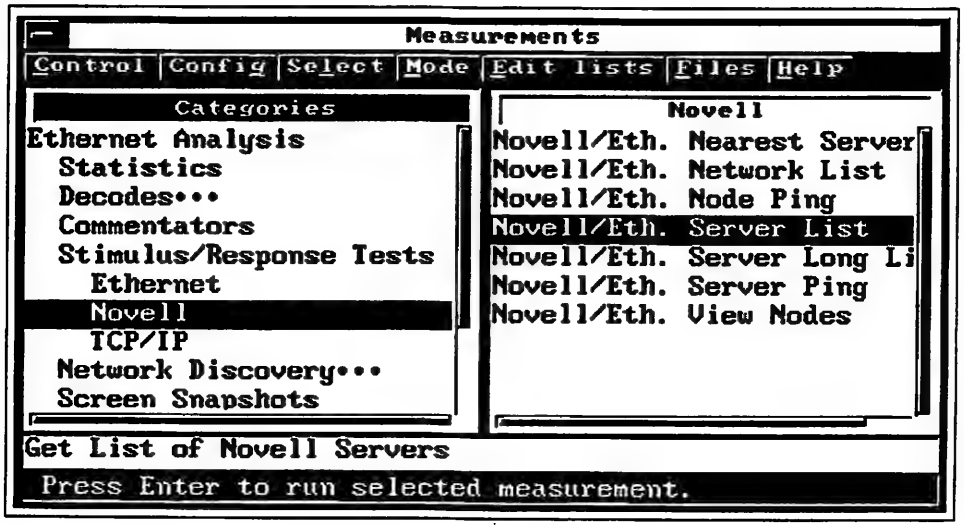
Results from running the PING test

6. Close the PING measurement by pressing **[F5]**.

Note: In the PING measurement configuration window, from the menu bar, Create | Create new measurement is available. You can create multiple copies of the PING measurement with custom configurations to test connectivity to special nodes on your network. This would save you time in re-configuring the measurement before running it.

Novell Tests

In the Advisor Measurements window, Stimulus/Response Tests category, there are several Novell stimulus/response tests available.



Novell Stimulus/Response Test category

Running these measurements requires a live network with Novell nodes. If you don't have access to a live network, review this section for information only.

The table on the following page describes each measurement available in the Novell Stimulus/Response Tests category:

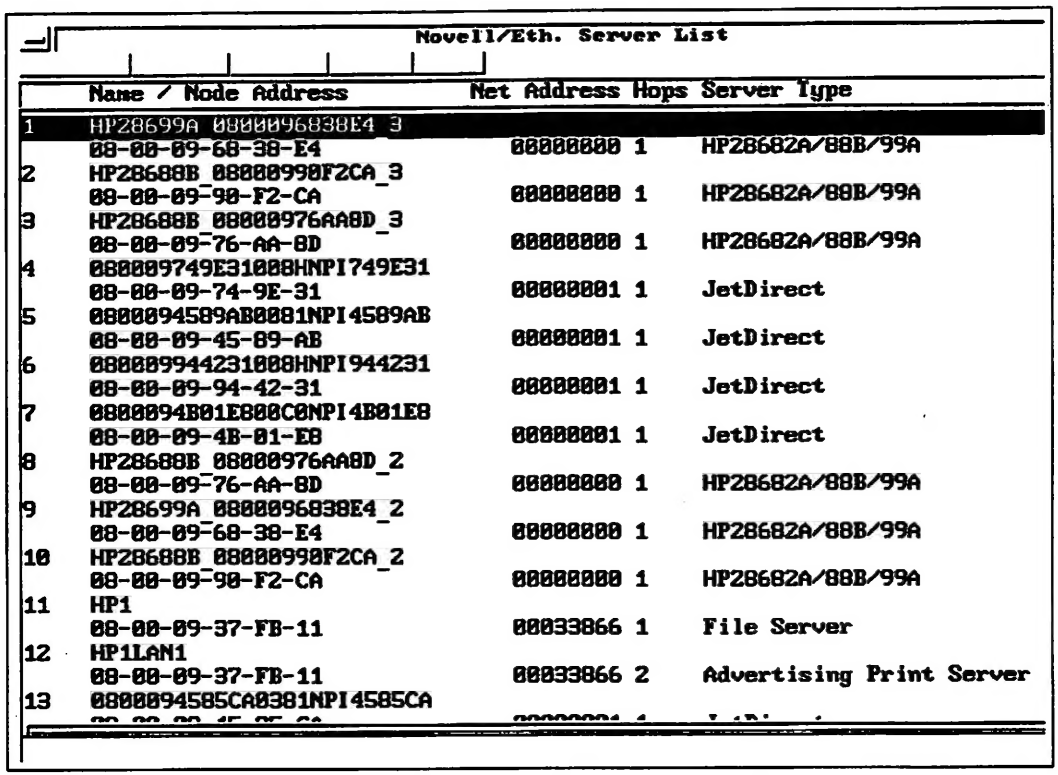
Novell Measurements	Function	Practical Applications
Nearest Server	Provides information about the nearest (in time) server of a specified type.	To determine: • Server's name and MAC address. • Server's network address. • Number of intermediate networks between the local segment and the segment where the server is located. • Type of server (file or print, for example) that responded.
Network List	Provides information about remote networks attached to the local segment.	To determine: • The network address assigned to the board of the responding node. • The node address that identifies the board in the responding node.
Node Ping	Provides information about a particular node.	To determine: • MAC Address of the node specified in the configuration window. • Number of components that perform Netware functions in the responding node. • Node name in the node/station list. • Type of component in the responding node. • Type of board used to access the network. • Network address assigned to the board of the responding node. • Node address assigned to the board of the responding node. • Number of packets sent and received.
Server List & Server Long List	Provides information about the servers available on the network under test.	To determine: • The name of the server and the MAC address of the node. • The network address assigned to the board of the responding server. • The number of intermediate networks between the local segment and the segment where the server is located. • The type of server (file or print, for example) that responded.

Server Ping	Provides information about a particular server.	To determine: • Name of the server that responded. • Name of this server from the node list. • Network address assigned to the board of the responding server. • Number of intermediate networks between the local segment and the segment where the server is located. • Number of packets sent and received.
View Nodes	Provides information about all Novell Netware nodes on the locally attached segment.	To determine: • MAC address of the responding node. • Socket on the node to which all SPX diagnostic requests are directed. • Number of boards that perform Netware functions in this node.

You may want to run all the above tests on your Novell network and review the results. For this chapter the Novell Server List measurement will be run and reviewed.

Novell Server List

1. From the Measurements window, Stimulus/Response Tests, Novell category, select **[Novell/Eth. Server List]** and press **[Enter]**. Press **[F4 | Z]** to zoom the Server List window. When the measurement has stopped running, press the **[Home]** key.



Novell/Eth. Server List

	Name / Node Address	Net Address	Hops	Server Type
1	HP28699A 080009683BE4_3			
	08-00-09-68-3B-E4	00000000	1	HP28682A/88B/99A
2	HP28688B 08000990F2CA_3			
	08-00-09-90-F2-CA	00000000	1	HP28682A/88B/99A
3	HP28688B 08000976AA8D_3			
	08-00-09-76-AA-8D	00000000	1	HP28682A/88B/99A
4	080009749E31088HNPI749E31			
	08-00-09-74-9E-31	00000001	1	JetDirect
5	080009458 9AB0081NPI4589AB			
	08-00-09-45-89-AB	00000001	1	JetDirect
6	080009944231088HNPI944231			
	08-00-09-94-42-31	00000001	1	JetDirect
7	080009 4B01E808C0NPI4B01E8			
	08-00-09-4B-01-E8	00000001	1	JetDirect
8	HP28688B 08000976AA8D_2			
	08-00-09-76-AA-8D	00000000	1	HP28682A/88B/99A
9	HP28699A 080009683BE4_2			
	08-00-09-68-3B-E4	00000000	1	HP28682A/88B/99A
10	HP28688B 08000990F2CA_2			
	08-00-09-90-F2-CA	00000000	1	HP28682A/88B/99A
11	HP1			
	08-00-09-37-FB-11	00033866	1	File Server
12	HP1LAN1			
	08-00-09-37-FB-11	00033866	2	Advertising Print Server
13	080009458 5CA0381NPI4585CA			

Responses from Novell Servers

2. A hardcopy of these results is available. From the Novell/Eth. Server List window menu bar, select **[Print | Print]**. If a printer is attached to the Internet Advisor, the list will be printed directly to the printer. If the Internet Advisor has been configured to print to a file, the File Manager window will appear, and the results of this measurement will be copied to an ASCII file.

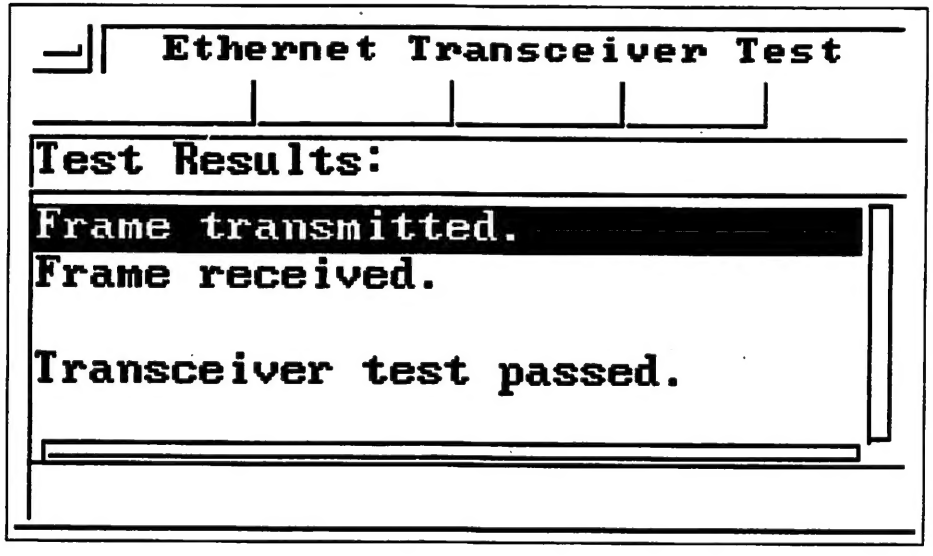
3. Press **[F5]** to close the Novell Server List measurement.

Ethernet Transceiver Test

The Ethernet Transceiver Test verifies that the Internet Advisor's transceiver is functioning normally by testing both the transmitter and receiver within the transceiver. This measurement sends a frame onto the network and then checks the Capture Buffer to see if the frame was captured. You can use this test to determine that the Internet Advisor is connected correctly to the network, that it is able to transmit and receive, and that the network is functioning properly. Be certain no filters are activated when you run this test.

1. From the Measurements window, Stimulus/Response Tests category, select **[Ethernet]**. Select the **[Ethernet Transceiver Test]** and press **[Enter]**.

2. The Ethernet Transceiver Test will run and verify whether the transceiver passed or failed.



Ethernet Transceiver Test – transceiver test passed.

3. Press **[F5]** to close the Ethernet Transceiver Test.

Chapter Notes

HEWLETT®
PACKARD

Reorder Part No.
Manual Part No.
5964-0547

5964-0547